adilson gonçalves

# introdução à álgebra

# ÍNDICE

# PREFÁCIO

Após experiências lecionando na Universidade de Brasília, e na Universidade Federal do Rio de Janeiro, pensei escrever um livro que viesse a ser um texto de Álgebra em nível de bacharelado (ou licenciatura) em Matemática.

Esse planejado texto deveria apresentar, entre outras coisas, um material elementar de dificuldade crescente, suficientemente interessante tanto para aqueles que fossem prosseguir nos estudos pós-graduados, como para aqueles que fossem se dedicar ao ensino.

Sem dúvida, as noções de conjunto, função, relação de equivalência, como também anéis, corpos, polinômios e grupos devem estar presentes em qualquer texto com esses objetivos. Escolhemos o Teorema Fundamental de Galois (característica zero) como principal objetivo a ser atingido pois, além de apresentar uma belíssima solução ao histórico problema sobre determinação de fórmulas para expressar raízes de um polinômio por meio de radicais, exige e aplica todas as noções elementares anteriormente apresentadas.

Abordaremos também os clássicos problemas da duplicação do cubo, da quadratura do círculo e da trisseção do ângulo, além de enunciarmos, sem demonstração, o famoso teorema de Gauss que caracteriza os números naturais $n \geq 3$ cujos polígonos regulares de n-lados no plano podem ser construidos por meio de régua e compasso.

As noções de conjunto, função e relação de equivalência foram intencionalmente apresentadas de modo sucinto no 1.º capítulo. Incluimos um grande número de exercícios complementares esperando que o aluno, com alguma orientação, entenda equilibradamente a importância dessas noções preliminares.

Considerando que a formalização envolvida na criação dos conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ cabe perfeitamente fora da seqüência de Álgebra (por exemplo, Matemática do Ensino Médio ou Evolução da Matemática, ou outro curso equivalente), penso que, como os analistas, os algebristas também deveriam usar e abusar da existência desses conjuntos numéricos, sem perder muito de seu tempo com essas formalizações. O teorema fundamental da álgebra é também admitido sem demonstração.

Dentro desse espírito, toda a teoria de Galois (chamada teoria de Galois elementar) foi desenvolvida para extensões $L \supset K$, onde

$\mathbb{C} \supset L \supset K \supset \mathbb{Q}$. O pouco de Álgebra Linear necessário na parte de extensões de corpos foi explicitado, embora nem tudo provado.

Nos Capítulos 2 e 4 é feito um estudo comparativo entre os anéis $\mathbb{Z}$ dos inteiros e $K[x]$ dos polinômios em uma variável com coeficientes em um corpo $K$. A teoria elementar de Anéis foi inserida no Capítulo 3 para evitar a repetição de tão evidentes analogias.

No Capítulo 5 incluimos importantes resultados a serem usados no capítulo final do texto, além de apresentarmos os anteriormente citados problemas clássicos e incluirmos um parágrafo sobre construção por meio de régua e compasso.

O Capítulo 6, sobre grupos, é o mais extenso embora isto não signifique que o lá apresentado deixe de ser elementar.

No último capítulo demonstramos os principais teoremas da Teoria de Galois sobre $\mathbb{Q}$ e discutimos o problema da solubilidade de equações polinomiais por meio de expressões radicais.

Agradeço a contribuição anônima dos meus alunos dos cursos de Álgebra e em especial agradeço ao corpo editorial do Projeto Euclides por esta oportunidade de realização.

Adilson Gonçalves

# INTRODUÇÃO

Dentro da história da Matemática o capítulo referente às equações polinomiais é certamente dos mais relevantes.

É conhecido que os Babilônios utilizavam, por volta de 1800 A.C., alguns métodos de resolução de equações do 2.º grau enquanto que os Egípcios, na mesma época, apenas possuiam métodos de resolução de equações do 1.º grau.

Os antigos gregos usavam os métodos das Construções Geométricas para resolverem algumas equações do 2.º grau e até alguns tipos de equações cúbicas. Dentro dessa linha, os gregos nos legaram os famosos problemas clássicos da "trisseção do ângulo", da "duplicação do cubo" e da "quadratura do círculo". A importância desses problemas está no fato que eles não podem ser resolvidos, geometricamente, por meio dos instrumentos régua (sem marcas) e compasso. Matemáticos de diferentes períodos contribuiram para mostrar a ligação desses problemas com a teoria das equações polinomiais, sendo então, todos respondidos negativamente [Bourbaki – Èlements d'Histoire des Mathematiques, Herman, Paris pag. 92].

Os Hindus, no início da era cristã, ao contrário dos Gregos, empregaram métodos aritméticos na resolução de equações, os quais foram desenvolvidos pelos Árabes. Um dos mais significantes resultados desse período Árabe é sem dúvida a solução da equação do 2.º grau $ax^2 + bx + c = 0$, cujas raízes são dadas pela conhecida fórmula

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Apesar de tudo, as resoluções algébricas para as equações cúbicas eram desconhecidas. No fim do século XV e início do século XVI os matemáticos italianos, principalmente de Bologna, descobriram que a solução da equação cúbica poderia ser reduzida àquelas dos seguintes tipos: $x^3 + px = q$, $x^3 = px + q$ e $x^3 + q = px$ (observe que essas distinções são decorrentes do não reconhecimento dos números negativos).

Scípio del Ferro, e mais tarde Niccolo Fontana (conhecido como Tartaglia), descobriram as soluções daquelas equações. Os argumentos de Tartaglia foram apropriados e divulgados por Cardano em Ars

Magna, 1545, que também divulgou o método de Ferrari de redução de uma equação do 4.º grau para uma de 3.º grau.

Vamos em seguida, apresentar um argumento (devido a Viète) para a solução de uma equação do 3.º grau.

Seja $F \supset \mathbb{Q}$ um corpo contendo o corpo dos números racionais e seja $f(x) = ax^3 + bx^2 + cx + d$ um polinômio de grau 3 com coeficientes em F. Substituindo $x$ por $y + h$ segue que o coeficiente de $y^2$ no polinômio $f(y + h)$ é $3ah + b$.

Escolhendo $h = \frac{-b}{3a}$ e dividindo a equação $f(x) = 0$ por $a$ teremos: $y^3 + py + q = 0$, $p, q \in F$.

Podemos admitir que esse polinômio é irredutível sobre $F$, pois de outro modo ele teria uma raiz em $F$ e as demais seriam raízes de um polinômio do 2.º grau com coeficientes em $F$.

Usando agora a substituição de Viète: $y = z + \frac{k}{z}$ a equação $y^3 + py + q = 0$ torna-se:

$$z^3 + 3zk + 3\frac{k^2}{z} + \frac{k^3}{z^3} + p \cdot z + p\frac{k}{z} + q = 0$$

Escolhendo $k = \frac{-p}{3}$ eliminamos os termos em $z$ e em $\frac{1}{z}$. Assim, a substituição $y = z - \frac{p}{3z}$ transforma a equação $y^3 + py + q = 0$ na equação $z^3 - \frac{p^3}{27z^3} + q = 0$ que vem a ser uma equação quadrática em $z^3$. Portanto,

$$z^3 = \frac{-q \pm \sqrt{-D/_{27}}}{2}, \text{ onde } D = -(4p^3 + 27q^2)$$

Agora se $z_1^3 = \frac{-q + \sqrt{-D/_{27}}}{2}$ e $z_2^3 = \frac{-q - \sqrt{-D/_{27}}}{2}$ teremos $(z_1 z_2)^3 = -\frac{p^3}{27}$ e daí segue que $z_1 z_2 = -\frac{p}{3} \cdot \lambda$ onde $\lambda$ é uma raiz cúbica da unidade.

Se $w = \cos\frac{2\pi}{3} + i \operatorname{sen}\frac{2\pi}{3} \in \mathbb{C}$ e substituindo, se necessário, $z_2$ por $wz_2$ ou $w^2 z_2$ podemos supor que $z_1 \cdot z_2 = -p/_3$ e as raízes cúbicas da equação $y^3 + py + q = 0$, serão:

$$y_1 = z_1 + z_2, y_2 = wz_1 + w^2 z_2 \text{ e } y_3 = w^2 \cdot z_1 + wz_2.$$

Assim,

$$y_1 = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

que vem a ser uma expressão obtida dos coeficientes através de repetidas adições, subtrações, multiplicações, divisões e extrações de raízes. Tais expressões são conhecidas como *expressões radicais.*

A equação geral do 4.º grau pode ser reduzida de modo análogo ao anterior para uma equação do tipo

(*) $$y^4 + py^2 + qy + r = 0$$

Seguindo um argumento de Descartes escolhemos $u$, $v$ e $w$ tais que (*) se reduz à equação $\left(y^2 + \frac{u}{2}\right)^2 - (vy + w)^2 = 0$ e daí seguem as relações:

(**) $$p = u - v^2,\ q = -2vw \text{ e } r = \frac{u^2}{4} - w^2.$$

As duas primeiras dessas relações nos dão: $u = p + v^2$ e $w = -q/_{2v}$, e substituindo-as em $r = \frac{u^2}{4} - w^2$ obtemos:

$v^6 + 2pv^4 + (p^2 - 4r)v^2 - q^2 = 0$, a qual vem a ser uma equação cúbica em $v^2$.

Assim, a equação do 4.º grau se reduz a uma equação cúbica e novamente temos que as raízes de uma equação do 4.º grau são dadas por uma expressão radical.

Ora, já que as raízes das equações de grau $\leq 4$ são expressões radicais, naturalmente a pergunta que segue é inevitável:

Será que as equações de grau 5 também são resolúveis por meio de expressões radicais?

Muitos matemáticos importantes atacaram o problema. Euler não conseguiu resolver o problema porém encontrou novos métodos para a resolução da equação do 4.º grau. Em 1770 Lagrange conseguiu uma etapa que iria contribuir bastante na solução do problema das equações de grau 5. Ele conseguiu unificar os argumentos nos casos das equações de grau 3 e 4 e mostrou por que o tal argumento falhava no caso do grau 5. A partir daí um sentimento de que a resposta para o grau 5 seria negativa tomou corpo entre os pesquisadores

da época. Ruffini, em 1813, tentou uma demonstração de tal impossibilidade mas seus argumentos tinham muitas falhas [Bourbaki – Elements d'Histoire des Mathematiques, Herman, Paris, pg. 103]. Finalmente em 1824 ABEL – provou que a "equação geral" de grau 5 não é resolúvel por meio de radicais. Porém, não ficou estabelecido quando um polinômio de grau $\geq 5$ é ou não "resolúvel por meio de radicais".

Em 1843 Liouville escreveu para a ACADEMIA DE CIÊNCIAS DE PARIS anunciando que os trabalhos deixados por Evariste Galois [1811-1832] continham uma solução que respondia precisamente quando um polinômio de grau $\geq 5$ é ou não "resolúvel por meio de radicais".

A solução apresentada por Galois, ao caracterizar os polinômios resolúveis por meio de radicais através de propriedades do grupo de automorfismos de um corpo, é considerada uma das mais belas páginas da História da Matemática e, uma das principais conquistas dessa ciência no século XIX.

No contexto desse livro introduzimos as noções algébricas necessárias à demonstração do teorema fundamental de Galois (sobre $\mathbb{Q}$) e provaremos que o polinômio $x^5 - 6x + 3$ não é "resolúvel por meio de radicais" pois o grupo de automorfismo do corpo de raízes desse polinômio é isomorfo ao grupo $S_5$ de todas as permutações de $\{1, 2, 3, 4, 5\}$, o qual não é um grupo solúvel no sentido definido por Galois.

CAPÍTULO I

# NOÇÕES PRELIMINARES

Incluiremos sob o título acima a terminologia de conjuntos e as noções de função e relação de equivalência. Deixaremos como exercícios muitas propriedades elementares envolvendo essas noções básicas.

## §1 Conjuntos

Entenderemos por *conjunto* uma qualquer coleção de objetos os quais chamaremos de *elementos* do conjunto. O *conjunto vazio* (isto é, o conjunto sem elementos) será denotado por $\emptyset$. Usaremos letras maiusculas para simbolizar conjuntos e minusculas para simbolizar elementos (as exceções ficarão claras no contexto do livro).

Se $x$ é um elemento do conjunto $A$ escreveremos $x \in A$ e leremos "$x$ *pertence* a $A$". Caso contrário escreveremos $x \notin A$ e leremos "$x$ *não pertence* a $A$".

Como primeiros exemplos de conjuntos podemos citar os conjuntos numéricos mais conhecidos, para os quais usaremos a seguinte nomenclatura:

$\mathbb{N} = \{0, 1, 2, \ldots, m, \ldots\}$ (números naturais)

$\mathbb{Z} = \{\ldots, -k, \ldots, -1, 0, 1, \ldots, m, \ldots\}$ (n.$^{os}$ inteiros)

$\mathbb{Q} = \left\{ m/n : \begin{matrix} m, n \in \mathbb{Z} \\ n \neq 0 \end{matrix} \right\}$ (números racionais)

$\mathbb{R} =$ (números reais, isto é, números racionais e números irracionais)

$\mathbb{C} = \left\{ a + bi : \begin{matrix} a, b \in \mathbb{R} \\ i = \sqrt{-1} \end{matrix} \right\}$

Sabemos, por exemplo, que $\sqrt{2} \in \mathbb{R}$ mas $\sqrt{2} \notin \mathbb{Q}$.

Quando todo elemento de um conjunto $A$ pertence a um conjunto $B$ dizemos que A *está contido* em $B$ ou $A$ é subconjunto de $B$ e denotamos por $A \subset B$. Consideraremos o conjunto $\emptyset$ contido em qualquer conjunto (raciocine por absurdo).

Dois conjuntos $A$ e $B$ são iguais se possuem os mesmos elementos. Assim temos claramente que $A = B$ se e somente se $A \subset B$ e $B \subset A$.

Se o conjunto $A$ não está contido no conjunto $B$ usaremos a notação $A \not\subset B$.

Em relação aos conjuntos numéricos acima temos

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

O conjunto dos elementos que pertencem simultâneamente a um conjunto $A$ e a um conjunto $B$ será denotado por

$A \cap B = \{x : x \in A \text{ e } x \in B\}$ e chamado de *interseção de A e B.*

O conjunto dos elementos que pertencem a um conjunto $A$ ou a um conjunto $B$ será denotado por

$A \cup B = \{x : x \in A \text{ ou } x \in B\}$ e chamado de *união de A e B.*

Claramente temos, quaisquer que sejam os conjuntos $A$ e $B$, as seguintes propriedades:

$$A \cap \varnothing = \varnothing, \quad A \cup \varnothing = A$$
$$A \cap B \subset A, \quad A \subset A \cup B.$$

Se $A \subset B$ também dizemos que $B$ *contém* $A$ e denotamos por $B \supset A$.

EXERCÍCIOS

1. Prove que quaisquer que sejam os conjuntos $A, B$ e $C$, tem-se:
   a) $A \subset A$
   b) Se $A \subset B$ e $B \subset C$ então $A \subset C$
   c) Se $A \subset B$ e $B \subset A$ então $A = B$.
2. Prove que quaisquer que sejam os conjuntos $A, B$ e $C$, tem-se:
   a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   c) $A \cup B = B \cup A$; $A \cap B = B \cap A$
   d) $A \cup (B \cup C) = (A \cup B) \cup C$; $A \cap (B \cap C) = (A \cap B) \cap C$
   e) $A \subset B$ se e somente se $A \cup B = B$ se e somente se $A \cap B = A$
3. Sejam $A, B \subset \Omega$. Definimos:

   $$C_\Omega A = \{x \in \Omega : x \notin A\}; \; A - B = \{a \in A : a \notin B\}$$

   Prove que:
   a) $C_\Omega(A \cup B) = C_\Omega A \cap C_\Omega B$; $C_\Omega(A \cap B) = C_\Omega A \cup C_\Omega B$
   b) $A \cap C_\Omega A = \varnothing$; $A \cup C_\Omega A = \Omega$
   c) $A - B = A \cap C_\Omega B$
   d) $C_\Omega(C_\Omega A) = A$

4. Sejam $A, B$ e $C \subset \Omega$. Demonstre as afirmações verdadeiras e dê contra-exemplos para as falsas:
   a) Se $A \subset B$ e $B \not\subset C$ então $A \not\subset C$
   b) $C_\Omega(A - B) = C_\Omega A \cap B$
   c) $A - (B - C) = A - (B \cup C)$
   d) $(A \cup B) - C = (A = C) \cup (B - C)$
   e) $(A - B) \cap C = (A \cap C) - (B \cap C)$

5. Dê, se possível, uma condição necessária e suficiente para que sejam verdadeiras as seguintes afirmações:
   Se $A, B$ são conjuntos então:
   a) $A \cup (B - A) = B$ b) $A - (A - B) = B$

6. Se $\Omega$ é um conjunto, definimos o conjunto das partes de $\Omega$ por $P(\Omega) = \{A : A \subset \Omega\}$. Calcule $P(\Omega)$ para os seguintes conjuntos $\Omega$ abaixo:
   a) $\Omega = \varnothing$ ; b) $\Omega = \{\varnothing\}$;
   c) $\Omega = \{\varnothing, 1, \{1\}\}$; d) $\Omega = \{x \in \mathbb{R} : x^2 < 2 \text{ e } x^2 - 4 > 0\}$.

7. Sejam $X$ e $Y$ conjuntos. Demonstre as afirmações verdadeiras e dê contra-exemplos para as falsas:
   a) Se $X \subset Y$ então $P(X) \subset P(Y)$
   b) Se $X \subset Y$ então $P(Y - X) = P(Y) - P(X)$.

8. Escreva os seguintes conjuntos $A$ como união de intervalos:
   a) $A = \{x \in \mathbb{R} : x^2 > 1 \text{ e } x^2 < 4\}$.
   b) $A = \{x \in \mathbb{R} : x^2 \geq 4 \text{ e } x^2 < 9\}$.
   c) $A = \{x \in \mathbb{R} : x^2 \geq 2 \text{ ou } x^2 \geq 1\}$.

. Sejam $A, B$ e $C$ conjuntos. É verdade em geral que
   a) $A \cup B = A \cup C \Rightarrow B = C$? b) $A \cap B = A \cap C \Rightarrow B = C$?
   Justifique!

10. Calcule $A \cap B$ nos seguintes casos:
   a) Se $A \cup B = A \cup C$ então $B = C$?
   b) Se $A \cap B = A \cap C$ então $B = C$?

## §2 Funções

Sejam $A$ e $B$ dois conjuntos. Chamamos de *função do conjunto A no conjunto B* a uma regra que a cada elemento de $A$ associa um único elemento de $B$, e denotamos simbolicamente por

$$\begin{aligned} f: A &\to B \\ a &\rightsquigarrow f(a) \end{aligned}$$

onde para cada $a \in A$ está associado um único $b = f(a) \in B$, através da regra que define $f$. Chamamos $A$ de *domínio da função* $f$ e $B$ de *contra-domínio da função* $f$.

Se $X \subset A$ e $f: A \to B$ denotamos por $f(X)$ ao conjunto $f(X) = \{f(x) : x \in X\} \subset B$ o qual chamamos de *imagem de* $X$ *pela* $f$. Detamos por Im $f$ ao conjunto $f(A)$ o qual chamamos de *Conjunto Imagem da* $f$. Dizemos que a função $f$ é *sobrejetiva* se $Im\ f = B$.

Observem que duas funções coincidem se e somente se possuem os mesmos domínios, os mesmos contradomínios e as mesmas regras. Por exemplo, as seguintes funções abaixo definidas são distintas apesar de possuirem o mesmo domínio e a mesma regra. Apenas a segunda delas e sobrejetiva.

$$f: \mathbb{R} \to \mathbb{R} \qquad\qquad g: \mathbb{R} \to \mathbb{R}^+$$
$$x \rightsquigarrow x^2 = f(x) \qquad x \rightsquigarrow x^2 = g(x)$$

onde $\mathbb{R}^+ = \{x \in \mathbb{R} : x \geq 0\}$.

Se $f: A \to B$ e $X \subset A$ denotaremos por $f|_X : X \to B$ a função cujo domínio é o conjunto $X$, cujo contra-domínio é o conjunto $B$ e cuja regra é a mesma de $f$, isto é, $f|_X(x) = f(x)$ qualquer que seja $x \in X$. Chamaremos $f|_X$ de *restrição de* $f$ *à* $X$.

Dizemos que uma função $f: A \to B$ é *injetiva* se quaisquer que sejam $x, y \in A$, se $x \neq y$ então $f(x) \neq f(y)$ (ou equivalentemente, quaisquer que sejam $x, y \in A$, se $f(x) = f(y)$ então $x = y$).

Se $f: A \to B$ é uma função simultaneamente *injetiva* e *sobrejetiva* dizemos que $f$ é uma função *bijetiva*.

Observe que das funções abaixo

$$f: \mathbb{R} \to \mathbb{R}^+ \quad , \quad g: \mathbb{R}^+ \to \mathbb{R}^+ \quad \text{e} \quad h: \mathbb{R} \to \mathbb{R}$$
$$x \rightsquigarrow x^2 = f(x) \qquad x \rightsquigarrow x^2 = g(x) \qquad x \rightsquigarrow x^3 = h(x)$$

apenas as duas últimas são bijetivas (desenhe o gráfico).

Se $f: A \to B$ é uma função e $y \in B$, denotamos por $f^{-1}(x)$ ao conjunto

$$f^{-1}(y) = \{x \in A : f(x) = y\}$$

o qual chamamos de *imagem inversa de* $y \in B$ *pela* $f$.

Observe que se $y \in B$ então $f^{-1}(y) \subset A$ e mais se $y \notin Im\, f$ então $f^{-1}(y) = \varnothing$.

Se $Y \subset B$ denotamos por $f^{-1}(Y)$ ao conjunto $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$ e chamamos tal conjunto de *imagem inversa de* $Y \subset B$ *pela* $f$.

Observe que em nossa terminologia temos,

$$\text{se } y \in B, \text{ então } f^{-1}(y) = f^{-1}(\{y\}).$$

Por exemplo, se $\begin{array}{l} f : \mathbb{R} \to \mathbb{R} \\ \quad x \rightsquigarrow \operatorname{sen} x \end{array}$ temos

$f^{-1}(1) = \left\{x = \dfrac{\pi}{2} + 2k\pi : k \in \mathbb{Z}\right\}$ e o conjunto $f^{-1}\left(\left\{0, \dfrac{1}{2}\right\}\right)$

é igual a:

$$\{x = k\pi : k \in \mathbb{Z}\} \cup \left\{x = \frac{\pi}{6} + 2k\pi : k \in \mathbb{Z}\right\} \cup \left\{x = \frac{5\pi}{6} + 2k\pi : k \in \mathbb{Z}\right\}$$

Se $f: A \to B$ e $g: B \to C$ são duas funções denotamos por $g \circ f : A \to C$ a função definida por $(g \circ f)(x) = g(f(x))$ qualquer que seja $x \in A$, a qual chamamos de *função composta de* $g$ *e* $f$.

A função $I_A : A \to A$ definida pela regra $I_A(x) = x$ qualquer que seja $x \in A$ é chamada de *função identidade de* $A$.

Observe que se $f : A \to B$ é uma função bijetiva então existe uma função $g: B \to A$ definida por: se $y \in B$, $g(y) = x$ onde $x$ é o único elemento de $A$ tal que $f(x) = y$ (o elemento $x$ existe pois $f$ é sobrejetiva e ele é único pois $f$ é injetiva).

É de fácil verificação as propriedades:

$$g \circ f = I_A \quad \text{e} \quad f \circ g = I_B$$

A função $g$ com as propriedades acima é dita ser a *função inversa* (claro que ela é única) *da função* $f$, e será denotada (não confundir com imagem inversa) por $g = f^{-1} : B \to A$.

Por exemplo, se $\begin{array}{l} f : \mathbb{R} \to \mathbb{R}^{\oplus} \\ \quad x \rightsquigarrow e^x \end{array}$ onde $\mathbb{R}^{\oplus} = \{x \in \mathbb{R} : x > 0\}$

então temos que $f$ é *bijetiva* e mais $\begin{array}{l} f^{-1} : \mathbb{R}^{\oplus} \to \mathbb{R} \\ \quad x \rightsquigarrow \log x \end{array}$

Se $\begin{array}{l} f : \mathbb{R} \to \mathbb{R} \\ \quad x \rightsquigarrow ax + b \end{array}$ com $a \neq 0$ temos que $f$ (uma reta) é

bijetiva e mais $f^{-1} : \mathbb{R} \to \mathbb{R}$ é tal que $f^{-1}(x) = \dfrac{1}{a}x - \dfrac{b}{a}$.

## EXERCÍCIOS

1. Seja $f: X \to Y$ uma função e sejam $A, A' \subset X$ e $B, B' \subset Y$. Prove que:
   a) $A \subset A' \Rightarrow f(A) \subset f(A)$; $B \subset B' \Rightarrow f^{-1}(B) \subset f^{-1}(B')$.
   b) $f(A \cup A') = f(A) \cup f(A')$; $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$
   c) $f(A \cap A') \subset f(A) \cap f(A')$. Se $f$ é injetiva vale a igualdade $f(A \cap A') = f(A) \cap f(A')$.
   d) $f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$.
   e) $f^{-1}(\underset{Y}{C}B) = \underset{X}{C}(f^{-1}(B))$.
   f) Se $f$ é bijetiva então $f(\underset{X}{C}A) = \underset{Y}{C}f(A)$.

2. Sejam as funções,

$$f: X \to Y,\ g: Y \to Z,\ h: Z \to W$$

   Então prove que:

$$h \circ (g \circ f) = (h \circ g) \circ f$$

3. Se $f: X \to Y$ é uma função bijetiva prove que existe uma única função $g: Y \to X$ tal que $f \circ g = I_Y$ e $g \circ f = I_X$.

4. Seja $f: X \to Y$ uma função. Prove que:
   a) $f$ é injetiva se e somente se existe $g: Y \to X$ tal que $g \circ f = I_X$ (i. e., $f$ é invertível à esquerda)
   b) $f$ é sobrejetiva se e somente se existe $h: Y \to X$ tal que $f \circ h = I_Y$ (i. e., $f$ é invertível à direita).

5. Seja $f: X \to Y$ uma função. Prove que:
   a) $f^{-1}(f(A)) \supset A$ qualquer que seja $A \subset X$; $f(f^{-1}(B) \subset B$, qualquer que seja $B \subset Y$.
   b) $f^{-1}(f(A)) = A$ qualquer que seja $A \subset X$ se e somente se $f$ injetiva.
   c) $f(f^{-1}(B)) = B$ qualquer que seja $B \subset Y$ se e somente se $f$ sobrejetiva.

6. Se $\Omega = \{1, 2, \ldots, n\}$ então denotamos por $S_n = \{f: \Omega \to \Omega : f \text{ bijetiva}\}$. Os elementos $\sigma$ de $S_n$ são também chamados de permutações de $\Omega$. Prove que: $S_n$ é um conjunto contendo $n!$ elementos.

7. Dê exemplos de funções $f, g: \mathbb{R} \to \mathbb{R}$ tais que $f \circ g \neq g \circ f$.

8. Seja $f: \{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$ uma função. Prove que:
   a) Se $f$ injetiva então $m \leq n$.

b) Se $f$ sobrejetiva então $m \geq n$.
c) Se $f$ bijetiva então $m = n$.

9. Seja $f: \{x_1, x_2, \ldots, x_n\} \to \{x_1, x_2, \ldots, x_n\}$ uma função. Prove que:
a) Se $f$ injetiva então $f$ sobrejetiva
b) Se $f$ sobrejetiva então $f$ injetiva.

. Seja $f: \mathbb{R} \to \mathbb{R}$ definida por:
$$f(x) = x^2 - 3x + 2.$$
Calcule:
$$f^{-1}(0), f^{-1}([0, \infty)), f^{-1}((-\infty, 0]) \text{ e } f^{-1}([1, 2]).$$

Seja $f: \mathbb{R} \to \mathbb{R}$ definida por:
$$f(x) = x^2 - 1.$$
Dê exemplo de conjunto não vazio $B \subset \mathbb{R}$ tal que:
a) $f^{-1}(B) = \varnothing$.
b) $f^{-1}(B)$ contém apenas um elemento.

12. Seja $f: X \to Y$ uma função e $M, N \subset Y$. Prove que:
$$f^{-1}(M - N) = f^{-1}(M) - f^{-1}(N).$$

13. Para cada uma das 8 leis abaixo especificadas explicite subconjuntos não vazios $X, Y \subset \mathbb{R}$ de modo que:
a) $y = f(x)$ defina uma função $f: X \to Y$.
b) $y = f(x)$ defina uma função $f: X \to Y$ sobrejetiva.
c) $y = f(x)$ defina uma função $f: X \to Y$ injetiva.
d) $y = f(x)$ defina uma função $f: X \to Y$ bijetiva.
onde as 8 leis são as seguintes: $y = x^4$; $y^2 = x$; $y^2 = 4 - x^2$; $y = e^x$; $y = \operatorname{sen} x$; $y = \operatorname{sen} e^x$; $y = \log \dfrac{1}{x - 3}$ e finalmente, $\dfrac{y^2}{16} = 1 - \dfrac{x^2}{9}$.

## §3 Relação de equivalência

Suponhamos que em um conjunto $A$ esteja definida uma relação entre pares de elementos de $A$. Se $x, x' \in A$ escreveremos $x \mathcal{R} x'$

se $x$ estiver relacionado com $x'$, e $x \not\mathcal{R} x'$ se $x$ não estiver relacionado com $x'$.

Por exemplo, se $A$ é o conjunto de retas do plano, ortogonalidade define uma relação $\mathcal{R}$ entre pares de elementos do conjunto $A$. Analogamente, paralelismo define uma relação no mesmo conjunto $A$.

Vamos agora definir o que vem a ser uma relação de equivalência em um conjunto $A$.

Seja $A$ um conjunto e seja $\mathcal{R}$ uma relação entre pares de elementos de $A$. Dizemos que $\mathcal{R}$ é uma *relação de equivalência em A* se as seguintes propriedades são verificadas quaisquer que sejam $x, x'$ e $x'' \in A$.

1. $x \mathcal{R} x$
2. Se $x \mathcal{R} x'$ então $x' \mathcal{R} x$
3. Se $x \mathcal{R} x'$ e $x' \mathcal{R} x''$ então $x \mathcal{R} x''$.

As propriedades acima são chamadas, respectivamente, reflexiva, simétrica e transitiva.

Observe que $\perp$ não é reflexiva nem transitiva. Se consideramos duas retas coincidentes como paralelas então paralelismo define uma relação de equivalência no conjunto de retas do plano.

Quando uma relação $\mathcal{R}$ em um conjunto $A$ for de equivalência vamos em geral usar a notação $\sim$ em vez de $\mathcal{R}$.

EXEMPLO 1. Seja $f: A \to B$ uma função e vamos definir uma relação de equivalência no domínio $A$ da $f$, do seguinte modo:

$$x, x' \in A, \ x \sim x' \ \text{se} \ f(x) = f(x')$$

A relação acima definida é claramente uma relação de equivalência no domínio $A$ da função $f$. Veremos mais adiante na Proposição 2 que qualquer relação de equivalência em um dado conjunto $A$ é proveniente de uma certa função como no Exemplo 1.

Seja $\sim$ uma relação de equivalência em um conjunto $A$ e seja $x \in A$. Vamos definir agora o que chamamos por *classe de equivalência* $\bar{x}$ do elemento $x$ em relação a $\sim$, a qual denotaremos por $\bar{x} = \{a \in A: a \sim x\}$.

Antes de enunciarmos a proposição 1 vamos explicitar o significado de alguns dos símbolos matemáticos mais utilizados.

$\exists$ – símbolo significando: "*Existe*"

$\forall$ – símbolo significando: "*Para todo(s)*, "*qualquer que seja*" *ou* "*quaisquer que sejam*"

$p \Rightarrow q$-símbolo significando: "*Se a proposição p é verdadeira então a proposição q também o é*".

$p \Leftrightarrow q$-símbolo significando: "*A proposição p é verdadeira se e somente se a proposição q é verdadeira*".

PROPOSIÇÃO 1. *Seja $\sim$ uma relação de equivalência em um conjunto A e sejam $x, y \in A$. Então*

1. $\bar{x} = \bar{y} \Leftrightarrow x \sim y$
2. $\bar{x} \neq \bar{y} \Rightarrow \bar{x} \cap \bar{y} = \emptyset$
3. $\bigcup_{x \in A} \bar{x} = A$

*Demonstração.* 1. ($\Rightarrow$): Sejam $x, y \in A$ e $\bar{x} = \bar{y}$. Vamos provar que $x \sim y$. De fato, pela definição de classe de equivalência temos,

$$\bar{x} = \{a \in A : a \sim x\} = \{z \in A : z \sim y\} = \bar{y}$$

e como $x \in \bar{x} = \bar{y}$ vem imediatamente que $x \sim y$.

($\Leftarrow$): Sejam $x, y \in A$ e $x \sim y$. Vamos provar que $\bar{x} = \bar{y}$ e para isso temos que provar que $\bar{x} \subset \bar{y}$ e $\bar{y} \subset \bar{x}$.

Vamos primeiramente provar que $\bar{x} \subset \bar{y}$. Seja $a$ um elemento arbitrário em $\bar{x}$, vamos provar que $a \in \bar{y}$.

Se $a \in \bar{x}$ temos $a \sim x$ e como $x \sim y$ (por hipótese) segue pela transitividade que $a \sim y$ e portanto $a \in \bar{y}$ como queríamos demonstrar.

Agora, se $x \sim y$ temos por simetria que $y \sim x$ e de modo análogo ao anterior chegamos à inclusão $\bar{y} \subset \bar{x}$ e daí segue que $\bar{x} = \bar{y}$ como queríamos demonstrar.

2. Suponhamos $x, y \in A$ e $\bar{x} \neq \bar{y}$. Se existisse algum elemento $a \in \bar{x} \cap \bar{y}$ teríamos $a \sim x$ e $a \sim y$ e, usando a simetria, seguiria $x \sim a$ e $a \sim y$ e pela transitividade teríamos $x \sim y$ e pelo item 1 dessa proposição $\bar{x} = \bar{y}$ o que contraria a nossa hipótese, assim $\bar{x} \cap \bar{y} = \emptyset$ como queríamos demonstrar.

3. Vamos provar que $\bigcup_{x \in A} \bar{x} = A$. De fato, temos primeiramente que $\bar{x} \subset A \; \forall x \in A$ e daí segue que $\bigcup_{x \in A} \bar{x} \subset A$. Reciprocamente temos que $x \in \bar{x} \; \forall x \in A$ e portanto segue que $A \subset \bigcup_{x \in A} \bar{x}$, e isto completa a demonstração da Proposição 1. ■

EXEMPLO 2. Seja $A = \mathbb{Z} = \{\ldots, -k, \ldots, -1, 0, 1, \ldots, m, \ldots\}$ e seja $n$ um número inteiro arbitrariamente fixado.

Vamos definir uma relação de equivalência em $\mathbb{Z}$ do seguinte modo: $x, x' \in \mathbb{Z}$, $x \sim x' \Leftrightarrow x - x'$ é um multiplo inteiro de $n$.

Claramente $\sim$ define uma relação de equivalência em $\mathbb{Z}$. Essa relação de equivalência recebe o nome de *congruência módulo n* e é geralmente indicada por $\equiv$ (mod $n$).

Assim, $x, x' \in \mathbb{Z}$, $x \equiv x' \pmod{n} \Leftrightarrow x - x'$ é um múltiplo inteiro de $n$.

Vamos agora calcular a classe $\bar{x}$, relativamente $a \equiv \pmod{n}$.

Se $x \in \mathbb{Z}$, $\bar{x} = \{a \in \mathbb{Z} : a \equiv x \pmod{n}\}$ e $a \in \bar{x} \Leftrightarrow a \equiv x \pmod{n} \Leftrightarrow$ $\Leftrightarrow a - x = k \cdot n$, $k \in \mathbb{Z} \Leftrightarrow a = x + k \cdot n$, $k \in \mathbb{Z}$.

Daí segue que: $\bar{x} = \{x + kn : k \in \mathbb{Z}\}$.

Observe que se $n = 0$ temos que $\bar{x} = \{x\}$ e que $\equiv$ (mod 0) nada mais é do que a relação de igualdade em $\mathbb{Z}$, e nesse caso existe um número infinito de classes $\bar{x} = \{x\}$ em $\mathbb{Z}$. Provaremos mais tarde que se $n > 0$ a relação $\equiv$ (mod $n$) nos fornece exatamente $n$ classes distintas quais sejam $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.

Assim, por exemplo, $\equiv$ (mod 3) nos fornece exatamente as classes $\bar{0}$, $\bar{1}$, $\bar{2}$ que são as classes dos números que deixam respectivamente restos zero, 1 e 2 na divisão por 3.

Agora vamos definir a noção de conjunto quociente.

Seja $\sim$ uma relação de equivalência em um conjunto $A$. Chamamos de *conjunto quociente de A pela relação de equivalência* $\sim$, e denotamos por $A/_{\sim}$, ao conjunto de todas as classes de equivalência relativamente a relação $\sim$.

Assim,

$$A/_{\sim} = \{\bar{x} : x \in A\}.$$

Na relação $\equiv$ (mod $n$), $n > 0$, em $\mathbb{Z}$ temos $\mathbb{Z}_{/\equiv (\mathrm{mod}\ n)} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ que também será representado por $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$.

Vamos enunciar agora o resultado que nos diz que toda relação de equivalência em um conjunto $A$ é proveniente (como no Exemplo 1) de uma função.

**PROPOSIÇÃO 2.** *Seja $\sim$ uma relação de equivalência em um conjunto A e seja $A/_{\sim} = \{\bar{x} : x \in A\}$ o conjunto quociente de A por $\sim$. Seja $\pi : A \to A/_{\sim}$ definida por $\pi(x) = \bar{x}$, $\forall\, x \in A$ ($\pi$ é chamada de* projeção canônica).

*Então a relação $\sim$ é proveniente da função $\pi$ como no Exemplo* 1.

*Demonstração.* De fato, basta observar pelo item 1 da Proposição 1 que se $x, y \in A$ temos, $x \sim y \Leftrightarrow \bar{x} = \bar{y} \Leftrightarrow \pi(x) = \pi(y)$ como queríamos demonstrar. ■

## §4 Produto cartesiano e operação binária em um conjunto

Vamos iniciar esse parágrafo introduzindo a noção de produto cartesiano de dois conjuntos. Sejam $A_1$ e $A_2$ dois conjuntos não vazios.

Definimos produto cartesiano dos conjuntos $A_1$ e $A_2$ como segue:

$$A_1 \times A_2 = \left\{(a_1, a_2)\colon \begin{matrix} a_i \in A_i \\ i = 1, 2 \end{matrix}\right\} \text{ onde,}$$

$$(a_1, a_2) = (b_1, b_2) \Leftrightarrow a_i = b_i,\ i = 1, 2.$$

Se $A_1 = A_2 = A$ denotamos por $A^2$ o produto $A_1 \times A_2$.

Usando a noção acima podemos reinterpretar a noção de relação de equivalência em um conjunto $A$.

Seja $A$ um conjunto não vazio e seja $\mathscr{R}$ um subconjunto do produto cartesiano $A^2$. $\mathscr{R}$ diz-se uma *relação (binária)* em $A$.

Usando a definição: se $a, b \in A$, "$a$ está relacionado com $b$" $\Leftrightarrow (a, b) \in \mathscr{R}$, podemos interpretar $\mathscr{R}$ como uma *relação entre pares de elementos de A*. Assim, para que a relação acima definida seja uma relação de equivalência é necessário e suficiente que: $\forall\, a, b, c \in A$

1) $(a, a) \in \mathscr{R}$ (reflexividade)
2) $(a, b) \in \mathscr{R} \Rightarrow (b, a) \in \mathscr{R}$ (simetria)
3) $(a, b) \in \mathscr{R}$, $(b, c) \in \mathscr{R} \Rightarrow (a, c) \in \mathscr{R}$ (transitividade)

Por exemplo, $\mathscr{R} = \{(a, a)\colon a \in A\}$ define a relação de igualdade no conjunto $A$, que é evidentemente uma relação de equivalência em $A$.

Se $A = \mathbb{R}$ então a interpretação geométrica das propriedades 1. e 2. nos diz que: o subconjunto $\mathscr{R}$ do pleano $\mathbb{R}^2$ contém a reta $y = x$ e é simétrico em relação a essa mesma reta, diagonal dos 1.º e 3.º quadrantes do plano.

Vamos agora definir a noção de operação (binária) em um conjunto não vazio $A$. Chamamos de *operação (binária)* em $A$ uma função

$$\mathscr{O}\colon A \times A \to A$$
$$(a, b) \rightsquigarrow \mathscr{O}(a, b) = a\mathscr{O}b.$$

A operação $\mathcal{O}$ diz-se *associativa* se $\forall\, a, b, c \in A$ tem-se $a\mathcal{O}(b\mathcal{O}c) = (a\mathcal{O}b)\mathcal{O}c$, e diz-se *comutativa* se $\forall\, a, b \in A$ tem-se $a\mathcal{O}b = b\mathcal{O}a$.

Como exemplos de operações associativas e comutativas temos a soma e o produto nos conjuntos numéricos $\mathbb{Z}$, $Q$, $\mathbb{R}$ e $\mathbb{C}$. É de fácil verificação que a composição de funções define uma operação não comutativa no conjunto $\mathscr{F}(\mathbb{R})$ de todas as funções $f: \mathbb{R} \to \mathbb{R}$.

Existe um ramo de álgebra que se dedica ao estudo das estruturas algébricas não associativas porém ele foge inteiramente aos nossos propósitos.

É fácil verificar que se $A = \{a, b\}$ e $\mathcal{O}$ é a operação definida por: $a\mathcal{O}b = b\mathcal{O}b = b$ e $a\mathcal{O}a = b\mathcal{O}a = a$ então $\mathcal{O}$ é uma operação em $A$ não comutativa e não associativa.

De modo análogo podemos introduzir a noção de produto cartesiano de mais de dois conjuntos e deixamos isso por conta do leitor.

## EXERCÍCIOS

1. Seja $A$ um conjunto não vazio e $P(A)$ o conjunto das partes de $A$.

   Dizemos que um conjunto não vazio $\mathbb{P} \subset P(A)$ é uma *partição do conjunto* $A$ se:

   (i) $\forall\, B_1, B_2 \in \mathbb{P}, B_1 \neq B_2 \Rightarrow B_1 \cap B_2 = \varnothing$

   (ii) $\bigcup_{B \in \mathbb{P}} B = A$.

   Prove que: se $x, y \in A$ e definimos $x \sim y \Leftrightarrow \exists\, B \in \mathbb{P}$ tal que $x, y \in B$, então $\sim$ define uma relação de equivalência no conjunto $A$. Mais ainda, $A/_\sim = \mathbb{P}$.

2. Seja $A$ um conjunto não vazio e $\sim$ uma relação de equivalência em $A$. Prove que $A/_\sim$ é uma partição do conjunto $A$.

3. Sejam $A_1, A_2, \ldots, A_n$ conjuntos. Definimos

   $$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i,\ i = 1, 2, \ldots, n\}$$

   onde,

   $$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \Leftrightarrow a_i = b_i,\ \ \forall i \in \{1, 2, \ldots, n\}.$$

   E chamamos $A_1 \times A_2 \times \ldots \times A_n$ de produto cartesiano dos conjuntos $A_1, A_2, \ldots, A_n$. Se $A = A_1 = A_2 = \ldots = A_n$ esse produto é denotado por $A^n$. Pergunta-se:

   É $P(\mathbb{R} \times \mathbb{R}) = P(\mathbb{R}) \times P(\mathbb{R})$? Justifique!

4. Se $A = \{0, 1\}$ e $B = \{0, 2, 3\}$. Calcule $P(A \times B)$ e $P(A) \times P(B)$.
5. Dê 3 exemplos de relações binárias no conjunto $\mathbb{R}$ dos números reais tais que no 1.º exemplo, a relação não seja reflexiva; no 2.º exemplo, não seja simétrica e no 3.º exemplo, não seja transitiva.
6. Seja $f: X \to Y$ uma função.
   Prove que:
   $$x_1, x_2 \in X,\ x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2)$$
   define uma relação de equivalência no conjunto $X$ (Nesse caso dizemos que $\sim$ é a relação de equivalência induzida por $f$).
7. Descreva as classes de equivalência e os conjuntos quocientes em relação a $\sim$ induzida pelas seguintes funções:
   a) $f: \mathbb{R} \to \mathbb{R}$
   $\quad x \rightsquigarrow f(x) = x^2 - 5x + 6$
   b) $f: \mathbb{Z} \to \mathbb{Z}$
   $\quad x \rightsquigarrow f(x) = x^2 - 7x + 10$
   c) $f: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$
   $\quad (x, y) \rightsquigarrow f(x, y) = y$
   d) $f: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$
   $\quad (x, y) \rightsquigarrow f(x, y) = +\sqrt{x^2 + y^2}$
8. Prove que $(x, y) \sim (x', y') \Leftrightarrow xy' = x'y$ define uma relação de equivalência no conjunto $\mathbb{Z} \times \mathbb{Z}^{\#}$ onde $\mathbb{Z}^{\#} = \mathbb{Z} - \{0\}$.
9. Dê exemplo de relações de equivalência $\sim$ em um conjunto $X$ tais que:
   a) $X/_\sim = \{X\}$
   b) $\bar{x} = \{x\}\ \forall x \in X$
   c) $X$ seja um conjunto infinito e o conjunto $X/_\sim$ contenha exatamente 11 elementos.
   d) $X$ seja um conjunto infinito e $X/_\sim$ também seja um conjunto infinito.
10. Teste a validade das propriedades reflexiva, simétrica e transitiva para as relações binárias definidas através dos seguintes subconjuntos $\Omega \subset \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ (plano real):
    a) $\Omega = \{(x, y) \in \mathbb{R}^2 : x \geq 0 \text{ e } y \geq 0\}$
    b) $\Omega = \{(x, y) \in \mathbb{R}^2 : y = x\}$
    c) $\Omega = \{(x, y) \in \mathbb{R}^2 : x \leq 0 \text{ e } y \geq 0\}$
    d) $\Omega = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$
    e) $\Omega =$ região dos pontos $(x, y)$ do plano tais que $1 \geq y - x \geq -1$

11. Uma relação $\leq$ entre pares de elementos de um conjunto $A$ diz-se uma *relação de ordem parcial em A* se:
   (i) $x \leq x \ \forall x \in \mathbb{R}$
   (ii) $x \leq y$ e $y \leq x \Rightarrow x = y \quad \forall x, y \in A$
   (iii) $x \leq y$ e $y \leq z \Rightarrow x \leq z \quad \forall x, y, z \in A$
   Uma relação de ordem parcial diz-se *total* ou *linear* se (iv) $\forall x, y \in A$, tem-se $x \leq y$ ou $y \leq x$.
   Prove que:
   a) $x \leq y \Leftrightarrow (y - x)$ é não negativo, define uma relação de ordem total no conjunto $\mathbb{Z}$.
   b) Se $A = \mathscr{F}(\mathbb{R})$ é o conjunto de todas as funções reais $f: \mathbb{R} \to \mathbb{R}$. Então:

$$f \leq g \Leftrightarrow f(x) \leq g(x) \ \forall x \in \mathbb{R}$$

   define uma relação de ordem parcial em $A$ que não é total em $A$.

# OS NÚMEROS INTEIROS

Neste capítulo apresentaremos uma visão algébrica dos números inteiros e para isso admitiremos conhecidas as propriedades elementares do conjunto $\mathbb{Z}$.

## §1 Propriedades elementares

No conjunto $\mathbb{Z}$ estão definidas as operações de soma e produto

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \quad (x, y) \rightsquigarrow x + y \qquad \text{e} \qquad \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \quad (x, y) \rightsquigarrow x \cdot y$$

as quais gozam das seguintes propriedades: $\forall x, y, z \in \mathbb{Z}$,

(i) $(x + y) + z = x + (y + z)$ (*associatividade* da soma)
(ii) $\exists\ 0 \in \mathbb{Z}$ tal que $x + 0 = 0 + x = x$ (existência do *elemento neutro*)
(iii) $\exists\ -x \in \mathbb{Z}$ tal que $x + (-x) = (-x) + x = 0$ (existência de *inverso aditivo* de cada elemento $x \in \mathbb{Z}$)
(iv) $x + y = y + x$ (*comutatividade* da soma)
(v) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (*associatividade* do produto)
(vi) $\exists\ 1 \in \mathbb{Z}$ tal que $x \cdot 1 = 1 \cdot x = x$ (existência da *unidade* em $\mathbb{Z}$)
(vii) $x \cdot y = y \cdot x$ (*comutatividade* do produto)
(viii) $x \cdot (y + z) = x \cdot y + x \cdot z$ (*distributividade* do produto em relação à soma)
(ix) $x \cdot y = 0 \Rightarrow x = 0$ ou $y = 0$ ($\mathbb{Z}$ não possui *divisores de zero*)

Veremos mais tarde estruturas algébricas que não satisfazem a propriedade (ix), isto é, estruturas com divisores de zero (que são elementos não nulos $a$ e $b$ tais que $a \cdot b = 0$). Usaremos a notação $xy$ em vez de $x \cdot y$, para simbolizar o produto dos elementos $x$ e $y$ em $\mathbb{Z}$.

Por possuir essas 9 propriedades acima dizemos que $\mathbb{Z}$ munido da soma e produto é um *domínio de Integridade.*

Mais adiante essa noção será definida com toda a generalidade.

## §2 Boa ordenação e algoritmo da divisão

Em $\mathbb{Z}$ existem as noções de "ordem" $\leq$ e de módulo $|\ |$, as quais admitiremos com algumas de suas propriedades básicas. Com o objetivo de demonstrar o algoritmo da divisão de Euclides iniciaremos esse parágrafo admitindo o princípio da boa ordenação em $\mathbb{Z}$.

*Princípio da boa ordenação*:

*Todo subconjunto não vazio* S *de* $\mathbb{Z}$ *de elementos não negativos possui um primeiro elemento, isto é,* $\exists\ x_0 \in S$ *tal que* $x_0 \leq x\ \forall x \in S$.

Vamos agora provar algumas propriedades de $\mathbb{Z}$ usando o princípio da boa ordenação.

PROPOSIÇÃO 1. *Não existe inteiro m tal que* $0 < m < 1$.

*Demonstração.* De fato, suponhamos por absurdo que existe tal $m \in \mathbb{Z}$, $0 < m < 1$.

Assim o conjunto $S = \{m \in \mathbb{Z} : 0 < m < 1\}$ é não vazio e pelo princípio da boa ordenação $\exists\ x_0 \in S$ tal que $x_0 \leq x\ \ \forall\ x \in S$. Como $x_0 \in S$ temos $0 < x_0 < 1$ e daí segue que $0 < x_0^2 < x_0 < 1$ e isto contradiz a minimalidade de $x_0 \in S$. ■

PROPOSIÇÃO 2 (Indução — 1.ª forma). *Suponhamos que seja dada uma afirmação* $a(n)$ *dependendo de* $n \in \mathbb{N}$ *tal que*:

(i) $a(0)$ é verdadeira.

(ii) Para $k \in \mathbb{N}$, $a(k+1)$ é verdadeira sempre que $a(k)$ for verdadeira.

Então, $a(n)$ é verdadeira $\forall\ n \in \mathbb{N}$.

*Demonstração.* Seja $S$ o conjunto dos inteiros $m \in \mathbb{N}$ tais que $a(m)$ seja falsa, e suponhamos que $S \neq \varnothing$. Pelo princípio da boa ordenação $\exists\ x_0 \in S$ tal que $x_0 \leq m\ \forall\ m \in S$. Como $a(0)$ é verdadeira, por hipótese temos que $0 \notin S$ e portanto $x_0 \geq 1$; mais ainda como $x_0 - 1 \notin S$ temos que $a(x_0 - 1)$ é verdadeira. Agora pela hipótese (ii) segue que $a(x_0) = a[(x_0 - 1) + 1]$ é verdadeira o que é uma contradição. Logo $S = \varnothing$ e a Proposição 2 está demonstrada. ■

**PROPOSIÇÃO 3** (Indução – 2.ª forma). *Suponhamos que seja dada uma afirmação $a(n)$ dependendo de $n \in \mathbb{N}$ tal que:*

(i) $a(0)$ é verdadeira.

(ii) Para cada inteiro $m > 0$, $a(m)$ é verdadeira sempre que $a(k)$ for verdadeira para $0 \leq k < m$.

Então, $a(n)$ é verdadeira $\forall\, n \in \mathbb{N}$.

*Demonstração.* Seja $S$ o conjunto dos inteiros $m \in \mathbb{N}$ tais que $a(m)$ seja falsa e suponhamos que $S$ é não vazio. Como acima, $\exists\, x_0 \in S$ tal que $x_0 \leq x\, \forall\, x \in S$, e pela hipótese (i) $x_0 > 0$. Portanto, $a(k)$ é verdadeira $\forall\, k$, $0 \leq k < x_0$ e (ii) nos dá uma contradição. ∎

Observe que as Proposições 2 e 3 poderiam ser enunciadas a partir do inteiro 1 em vez de zero e nesse caso a hipótese (i) seria a(1) é verdadeira. As mesmas demonstrações funcionam com as devidas modificações.

**TEOREMA 1** (Algoritmo da Divisão). *Sejam $n$, $d \in \mathbb{N}$ e $d > 0$. Então existem únicos $q$, $r \in \mathbb{N}$, tais que* $n = q\,d + r$ e $0 \leq r < d$.

*Demonstração.* Provaremos a existência usando indução (2.ª forma) sobre $n$.

Se $n < d$ existem $q = 0$, $r = n$, assim podemos assumir $n \geq d > 0$. Então temos $0 \leq n - d < n$ e pela hipótese (ii) de indução (2.ª forma) segue que $\exists\, q_1, r \in \mathbb{N}$ tais que $n - d = q_1\, d + r$ onde $0 \leq r < d$ e daí segue que $n = (q_1 + 1)d + r$ onde $0 \leq r < d$. Assim existem $q = q_1 + 1$ e $r \in \mathbb{N}$ como queríamos demonstrar.

Provaremos agora a unicidade. Suponhamos que existam $q_1$, $r_1$, $q_2, r_2 \in \mathbb{N}$ tais que $n = q_1 d + r_1, 0 \leq r_1 < d$ e $n = q_2 d + R_2, 0 \leq r_2 < d$.

Daí segue que, $q_1 d + r_1 = q_2 d + r_2$ onde $0 \leq r_1 < d$ e $0 \leq r_2 < d$. Como $d > 0$ é suficiente provarmos que $r_1 = r_2$ pois nesse caso teríamos $q_1 d = q_2 d$ ou seja $q_1 = q_2$. Suponhamos por absurdo que $r_1 \neq r_2$, por exemplo $r_1 > r_2$. Nesse caso teríamos

$$0 < r_1 - r_2 = (q_2 - q_1)d.$$

Mas também $r_1 - r_2 < d$ pois $r_1 < d$ e $r_2 < d$, e daí segue que:

$$0 < r_1 - r_2 = (q_2 - q_1)d < d$$

o que é um absurdo, e isto termina a demonstração do Teorema 1. ∎

Observem que na demonstração do Teorema 1 a afirmação $a(n)$ usada na indução foi a seguinte:
"$\exists\, q, r \in \mathbb{N}$ tais que $n = qd + r$, onde $0 \leq r < d$".

EXERCÍCIOS

1. Enuncie as Proposições 2 e 3 a partir do inteiro 1 e prove por indução as seguintes fórmulas:

   a) $1 + 2 + \ldots + n = \dfrac{n(n+1)}{2}$ $\forall\, n \geq 1$ inteiro.

   b) $1 + 4 + \ldots + n^2 = n(n+1)\dfrac{(2n+1)}{6}$ $\forall\, n \geq 1$ inteiro.

   c) $1 + 8 + \ldots + n^3 = \left[\dfrac{n(n+1)}{2}\right]^2$

   d) $1 + 3 + \ldots + (2n-1) = n^2$

2. Prove que o conjunto $S = \{m \in \mathbb{Z} : 7 < m < 8\}$ é vazio.

3. Se $m, n \in \mathbb{N}$ e $n \geq m$ definimos $\begin{pmatrix} n \\ m \end{pmatrix} = \dfrac{n!}{(n-m)!\, m!}$ onde $n! = n(n-1)\ldots 3 \cdot 2 \cdot 1$ se $n \geq 1$ e $0! = 1$. Prove (por indução sobre $n$) a seguinte fórmula onde $n \geq m \geq 1$ são inteiros:

$$\begin{pmatrix} n \\ m-1 \end{pmatrix} + \begin{pmatrix} n \\ m \end{pmatrix} = \begin{pmatrix} n+1 \\ n \end{pmatrix}$$

4. Se $x, y \in \mathbb{Z}$ e $n \in \mathbb{N}$. Prove por indução sobre $n$ que:

$$(x+y)^n = x^n + \begin{pmatrix} n \\ 1 \end{pmatrix} x^{n-1} y + \ldots + \begin{pmatrix} n \\ i \end{pmatrix} x^{n-i} y^i + \ldots + y^n$$

   (*Sugestão*: Use o exercício 3)

5. Seja $a \neq 0 \in \mathbb{Z}$ e $m \in \mathbb{N}$. Definimos potencia não negativa de $a$ do seguinte modo:

   $a^0 = 1$, $a^1 = a$, $a^m = \underbrace{a \cdot a \ldots a}_{m \text{ vezes}}$ se $m \geq 2$.

Prove que:
a) $a^m \cdot a^n = a^{m+n}$ $\forall m, n \in \mathbb{N}$
b) $(a^m)^n = a^{m \cdot n}$ $\forall m, n \in \mathbb{N}$.

6. Prove, por indução sobre $n$, que $n^3 + 2n$ é sempre divisível por 3.
7. Se $A = \{1, 2, \ldots, n\}$ denotamos por $P(A)$ o conjunto das partes de $A$, i.e., $P(A) = \{B : B \subset A\}$. Prove que $|P(A)| = 2^n$, onde $|X|$ denota o número de elementos do conjunto $X$.
8. Se $n$ é um natural ímpar. Prove que $n^3 - n$ é sempre divisível por 24.

## §3 Ideais e M.D.C.

Neste parágrafo vamos provar a existência de Máximo Divisor Comum em $\mathbb{Z}$ e para isto vamos definir a noção de Ideal do domínio $\mathbb{Z}$.

Seja $J \subset \mathbb{Z}$. Dizemos que $J$ é um *ideal de* $\mathbb{Z}$ se as seguintes condições são satisfeitas:

(i) $0 \in J$
(ii) $x, y \in J \Rightarrow x + y \in J$
(iii) $x \in J \Rightarrow -x \in J$
(iv) $r \in \mathbb{Z},\ x \in J \Rightarrow r x \in J$.

Observe que as condições (i), (ii) e (iii) poderiam ser substituidas pelas condições

(i)′ $J \neq \varnothing$
(ii)′ $x, y \in J \Rightarrow x - y \in J$.

De fato, se $x \in J \neq \varnothing$ então $0 = x - x \in J$ por (ii)′. Agora se $x \in J$ então $-x = 0 - x \in J$, e finalmente se $x, y \in J$ temos $x, -y \in J$ e daí segue $x + y = x - (-y) \in J$ como queríamos demonstrar.

EXEMPLO 1. Se $n$ é um número inteiro qualquer, então o conjunto de todos os múltiplos inteiros de $n$ é um Ideal de $\mathbb{Z}$.

De fato, seja $J = \{nk : k \in \mathbb{Z}\}$ o conjunto de todos os múltiplos inteiros de $n$. Então segue que:

(i)′ $0 = n \cdot 0 \in J \neq \varnothing$
(ii)′ $x = nk,\ y = n r \in J \Rightarrow x - y = n(k - r) \in J$
(iv) $r \in \mathbb{Z},\ x = nk \in J \Rightarrow r x = x r = n(kr) \in J$

Observe que no Exemplo 1, se $n = 0$ temos que $J = \{0\}$ é um ideal de $\mathbb{Z}$, e se $n = 1, J = 1 \cdot \mathbb{Z} = \mathbb{Z}$ é também um ideal de $\mathbb{Z}$. Esses ideais são chamados de *ideais triviais de* $\mathbb{Z}$. Se $J$ é um ideal de $\mathbb{Z}$ tal que $\{0\} \neq J \neq \mathbb{Z}$

dizemos que $J$ é um *ideal próprio* de $\mathbb{Z}$. Por exemplo $J = 2 \cdot \mathbb{Z} = \{2 \cdot k : k \in \mathbb{Z}\}$ é um ideal próprio de $\mathbb{Z}$. É usual a notação $n \cdot \mathbb{Z}$ para o ideal dos múltiplos inteiros de $n$.

EXEMPLO 2. Se $n_1, n_2, \ldots, n_k$ são números inteiros quaisquer então o conjunto de todos os números inteiros da forma $n_1r_1 + \ldots + n_kr_k$, onde $r_1, \ldots, r_n$ são inteiros, é um ideal de $\mathbb{Z}$.

De fato, seja $J = \{n_1r_1 + \ldots + n_kr_k : r_i \in \mathbb{Z}\}$. Então segue que:

(i)′ $0 = n_1 \cdot 0 + \ldots + n_k \cdot 0 \in J \neq \emptyset$

(ii)′ $x = n_1r_1 + \ldots + n_kr_k,\ y = n_1s_1 + \ldots + n_ks_k \in J \Rightarrow$
$\Rightarrow x - y = n_1(r_1 - s_1) + \ldots + n_k(r_k - s_k) \in J$

(iv) $r \in \mathbb{Z},\ x = n_1r_1 + \ldots + n_kr_k \in J \Rightarrow$
$\Rightarrow r\,x = x\,r = n_1(r_1r) + \ldots + n_k(r_kr) \in J.$

É usual a notação $n_1\mathbb{Z} + \ldots + n_k\mathbb{Z}$ para o ideal $J$.

O Ideal $n \cdot \mathbb{Z}$ dos múltiplos do inteiro $n$ é também chamado de *Ideal principal gerado por* $n$, enquanto o ideal $n_1\mathbb{Z} + \ldots + n_k\mathbb{Z}$ é chamado de *ideal gerado* pelos inteiros $n_1, \ldots, n_k$.

Antes de demonstrar a existência do Máximo divisor comum em $\mathbb{Z}$ provaremos o seguinte Teorema:

TEOREMA 2 ($\mathbb{Z}$ é um domínio principal). *Todo ideal de* $\mathbb{Z}$ *é principal.*

*Demonstração.* Seja $J$ um ideal de $\mathbb{Z}$. Se $J = \{0\}$ então $J$ é um ideal principal gerado por 0.

Suponhamos que $J \neq \{0\}$. Assim existe $0 \neq x \in J$ e pela propriedade (iii) temos $-x \in J$ e portanto $|x| \in J$, $|x| > 0$, ou seja, o conjunto $S$ dos inteiros $> 0$ pertencentes à $J$ é não vazio. Pelo princípio da boa ordenação $\exists\, d \in J$, tal que $d$ é o menor inteiro $> 0$ em $J$. Vamos provar que $d \cdot \mathbb{Z} = J$.

Claramente $d \cdot \mathbb{Z} \subset J$ pois se $d \in J$ e $n \in \mathbb{Z}$ então $d\,r = r\,d \in J$ por (iv). Assim é suficiente provarmos que $J \subset d \cdot \mathbb{Z}$.

Seja $x \in J$. Pela propriedade (iii) temos que $|x| \in J$ e pelo Algoritmo da divisão temos que $\exists\, q, r \in \mathbb{Z}$ tais que:

$$|x| = q\,d + r \quad \text{onde} \quad 0 \leq r < d.$$

Daí segue que $0 \leq r = |x| - q\,d < d$. Como $|x|$ e $q \cdot d \in J$ temos $r \in J$ e $0 \leq r < d$.

Pela minimalidade de $d$ segue que $r = 0$ e portanto $|x| = q \cdot d \in d \cdot \mathbb{Z}$ e novamente por (iii) teremos $x \in d \cdot \mathbb{Z}$ (desde que $d \cdot \mathbb{Z}$ é também um ideal), como queríamos demonstrar. ■

TEOREMA 3 (Existência de M.D.C. em $\mathbb{Z}$). *Sejam* $n_1\ n_2, \ldots, n_k$ *inteiros não nulos e seja* $J = n_1 \mathbb{Z} + \ldots + n_k\mathbb{Z}$ *o ideal gerado por* $n_1, \ldots, n_k$.

Se $d \in \mathbb{Z}$ é tal que $J = d \cdot \mathbb{Z}$ então são válidas as seguintes afirmações:

(a) $\exists\, r_1, \ldots, r_k \in \mathbb{Z}$ tais que $d = n_1 r_1 + \ldots + n_k r_k$

(b) $d$ é um divisor comum de $n_1, \ldots, n_k$.

(c) Se $d'$ é um divisor comum qualquer de $n_1, \ldots, n_k$ então $d'$ é também um divisor de $d$.

*Demonstração.* (a) Sai imediatamente da igualdade $d \cdot \mathbb{Z} = n_1\mathbb{Z} + \ldots + n_k\mathbb{Z}$ e do fato $d \in d \cdot \mathbb{Z}$.

(b) Seja $i \in \{1, \ldots, k\}$ e $d \cdot \mathbb{Z} = n_1\mathbb{Z} + \ldots + n_k\mathbb{Z}$ então é claro que,

$$n_i \in n_i \cdot \mathbb{Z} \subset n_1\, \mathbb{Z} + \ldots + n_i\, \mathbb{Z} + \ldots + n_k\, \mathbb{Z} = d \cdot \mathbb{Z}$$

e portanto $\exists\, r_i \in \mathbb{Z}$ tal que $n_i = d\, r_i$, isto é, $d$ é um divisor de cada $n_i$, $i = 1, \ldots, k$.

(c) Seja $d'$ um divisor comum qualquer de

$$n_1, n_2, \ldots, n_k. \text{ Assim, } \exists\, r_i, i = 1, 2, \ldots, k$$

tal que $n_i = d' \cdot r_i$, ou seja: $n_i\mathbb{Z} \subseteq d'\,\mathbb{Z}\ \forall\, i \in \{1, 2, \ldots, k\}$ e daí segue imediatamente que:

$$n_1\mathbb{Z} + \ldots + n_k\mathbb{Z} = d\mathbb{Z} \subseteq d'\mathbb{Z}$$

e portanto: $d \in d'\,\mathbb{Z}$, isto é, $\exists\, r \in \mathbb{Z}$ tal que $d = d'\, r$ e isto demonstra o item c) do Teorema. ■

Um número satisfazendo as condições dos itens b) e c) do Teorema 3 diz-se *um M.D.C. de* $n_1, n_2, \ldots, n_k$ *em* $\mathbb{Z}$.

Observe que se $d$ é um M.D.C. de $n_1$, $n_2, \ldots, n_k$ em $\mathbb{Z}$ então $-d$ também o é pois $d\,\mathbb{Z} = -d\,\mathbb{Z}$. É claro também que em $\mathbb{Z}$ existe um único M.D.C. positivo de $n_1, n_2, \ldots, n_k$, (e nesse caso dizemos o M.D.C. de $n_1, n_2, \ldots, n_k$) o qual denotaremos por M.D.C. $\{n_1, \ldots, n_k\}$. Assim, pelo item a) do Teorema 3 se $d =$ M.D.C. $\{n_1, \ldots, n_k\}$ então existem inteiro $n_1, \ldots, r_k$ tais que $d = n_1 r_1 + \ldots + n_k r_k$.

Se $1 = \text{M.D.C. } \{n_1, \ldots, n_k\}$ dizemos que $n_1, \ldots, n_k$ são *relativamente primos em* $\mathbb{Z}$ e pela observação anterior $\exists\, r_1, \ldots, r_k$ tal que:

$$1 = n_1 r_1 + \ldots + n_k r_k.$$

## EXERCÍCIOS

1. Definindo,

$$| \ |: \mathbb{Z} \to \mathbb{N}$$

$$a \rightsquigarrow |a| = \begin{cases} a & \text{se } a \geq 0 \\ -a & \text{se } a \leq 0 \end{cases}$$

Prove que:

a) $|a| \geq 0 \quad \forall a \in \mathbb{Z}; \quad |a| = 0 \Leftrightarrow a = 0$

b) $|a + b| \leq |a| + |b| \quad \forall a, b \in \mathbb{Z}$

c) $|a \cdot b| = |a| \cdot |b| \quad \forall a, b \in \mathbb{Z}$

d) $|a - b| \geq ||a| - |b|| \quad \forall a, b \in \mathbb{Z}.$

2. Dados $a, b \in \mathbb{N} - \{0\}$. Aplicando sucessivamente o algoritmo de Euclides temos:

$a = q_0 b + r_1, \quad 0 \leq r_1 < b$

$b = q_1 r_1 + r_2, \quad 0 \leq r_2 < r_1$

$r_1 = q_2 r_2 + r_3, \quad 0 \leq r_3 < r_2$

$\vdots$

$r_k = q_{k+1} r_{k+1} + r_{k+2}, \quad 0 \leq r_{k+2} < r_{k+1}$

como $r_1 > r_2 > r_3 > \ldots > r_k > r_{k+1} \geq 0$ temos que existe um primeiro inteiro $s$ tal que $r_{s+1} = 0$. Prove que $r_s = \text{M.D.C. } \{a, b\}$.

3. Usando o exercício anterior. Calcule M.D.C. $\{180,252\}$.

4. Calcule $r$ e $s \in \mathbb{Z}$ tais que M.D.C. $\{a, b\} = ra + sb$ nos seguintes casos:

a) $a = 21$ ; $\quad b = 35.$

b) $a = 11$ ; $\quad b = 15.$

c) $a = 180$; $\quad b = 252.$

5. Prove que se $a, b \in \mathbb{Z}$ e $\exists\, r, s \in \mathbb{Z}$ tais que $ra + sb = 1$ então M.D.C. $\{a, b\} = 1$.

6. Prove que se $a > 0$ e $b, c \in \mathbb{Z}$ então,

$$\text{M.D.C. } \{ab, ac\} = a \cdot \text{M.D.C. } \{b, c\}.$$

7. Demonstrar que:

Se M.D.C. $\{a, n\} =$ M.D.C.$\{a, m\} = 1$ então M.D.C. $\{a, mn\} = 1$.

8. Demonstrar o algoritmo da divisão quando o divisor $d$ é negativo. Que nesse caso o resto $r$ satisfaz $0 \leq r < |d|$.
9. Quais dos seguintes subconjuntos $I$ de $\mathbb{Z}$ abaixo são ideais de $\mathbb{Z}$:
   a) $I = \{m \in \mathbb{Z}$ : alguma potência de $m$ é divisível por $64\}$.
   b) $I = \{m \in \mathbb{Z} : \text{M.D.C.}\{7, m\} = 1\}$.
   c) $I = \{m \in \mathbb{Z} : m$ é um divisor de $24\}$.
   d) $I = \{m \in \mathbb{Z} : 24$ é um divisor de $m\}$.
   e) $I = \{m \in \mathbb{Z} : 6 \backslash m$ e $24 \backslash m^2\}$.
   f) $I = \{m \in \mathbb{Z} : 21 \cdot m$ é divisível por $9\}$.
10. Se $I_1, I_2, \ldots, I_r$ são ideais de $\mathbb{Z}$. Prove que:
    a) $I_1 \cap I_2 \cap \ldots \cap I_r$ é um ideal de $\mathbb{Z}$.
    b) $I_1 + I_2 + \ldots + I_r = \{x_1 + x_2 + \ldots + x_r : x_j \in I_j\}$, $j = 1, 2, \ldots, r\}$, é um ideal de $\mathbb{Z}$.
11. Identifique $q$ tal que $\mathbb{Z}_m \cap \mathbb{Z}_n = \mathbb{Z} \cdot q$.
12. Se $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_i \subseteq I_{i+1} \subseteq \ldots$ são ideais de $\mathbb{Z}$. Prove que: $\bigcup_{r=1}^{\infty} I_r = J$ é um ideal de $\mathbb{Z}$.
13. Prove que: se $I \nsubseteq J$ e $J \nsubseteq I$ onde $I$ e $J$ são ideais de $\mathbb{Z}$ então $I \cup J$ não é um ideal de $\mathbb{Z}$.
14. Seja $I$ um ideal de $\mathbb{Z}$. Prove que se $1 \in I$ então $I = \mathbb{Z}$.

## §4 Números primos e Ideais maximais

Sejam $d$ e $n$ elementos de $\mathbb{Z}$. Dizemos que $d$ é um *divisor de n* em $\mathbb{Z}$, e escrevemos $d \backslash n$, se $\exists\, b \in \mathbb{Z}$ tal que $n = d\,b$ (nesse caso também dizemos que $n$ é um *multiplo de d*). Dizemos que um inteiro $p$ é um *número primo de* $\mathbb{Z}$ se $p \neq \pm 1$ e os únicos divisores de $p$ são $\pm 1$ e $\pm p$. Observe que esta definição de número primo é equivalente a seguinte: $p \in \mathbb{Z}$ é um número primo se $p \neq \pm 1$ e toda vez que $p = a\,b$, com $a, b \in \mathbb{Z}$, então $a = \pm 1$ ou $a = \pm p$.

Vamos agora provar duas proposições que nos serão úteis no próximo parágrafo.

**PROPOSIÇÃO 4.** *Se um número primo p não é um divisor de um número inteiro n, então $\exists\, r, s \in \mathbb{Z}$ tais que $rp + sn = 1$.*

*Demonstração.* Seja $d > 0$ o M.D.C. de $p$ e $n$, isto é, $d = \text{M.D.C.}\{p, n\}$. Pela definição de M.D.C. temos que $d$ é um divisor de $p$ e portanto $d = 1$ ou $p$. Mas como $d \backslash n$ e $p$ não divisor de $n$, temos que $d = 1$ e a proposição segue pois $1 \in d \cdot \mathbb{Z} = p \cdot \mathbb{Z} + n\mathbb{Z}$. ■

PROPOSIÇÃO 5. *Todo número primo que divide um produto divide pelo menos um dos fatores.*

*Demonstração.* Suponhamos que $p \backslash ab$ e que $p$ não é divisor de $a$ e vamos provar que $p \backslash b$. De fato, pela proposição 1 segue que $\exists\, r, s \in \mathbb{Z}$ tais que,

$$p \cdot r + a \cdot s = 1$$

e multiplicando ambos os membros da igualdade por $b$, temos que,

$$p \cdot (r \cdot b) + (a \cdot b) \cdot s = b$$

e portanto $p \backslash b$. ■

Vamos agora definir a noção de *ideal maximal em* $\mathbb{Z}$ e relaciona-la com números primos.

Um ideal $\mathcal{M}$ de $\mathbb{Z}$ diz-se um *ideal maximal em* $\mathbb{Z}$ se $\mathcal{M} \neq \mathbb{Z}$ e se $J$ é um ideal de $\mathbb{Z}$ tal que

$$\mathcal{M} \subset J \subset \mathbb{Z} \text{ então } J = \mathcal{M} \text{ ou } J = \mathbb{Z}.$$

Em outras palavras, um ideal $\mathcal{M} \neq \mathbb{Z}$ de $\mathbb{Z}$ é dito maximal se os únicos ideais de $\mathbb{Z}$ contendo $\mathcal{M}$ são $\mathcal{M}$ e $\mathbb{Z}$.

TEOREMA 4. *Se $p \in \mathbb{Z}$ e $J = p \cdot \mathbb{Z}$ então as seguintes condições são equivalentes*:

(i) $p$ é um número primo.

(ii) $J = p \cdot \mathbb{Z}$ é um ideal maximal em $\mathbb{Z}$.

*Demonstração.* (i) $\Rightarrow$ (ii): Seja $p$ um número primo e $J = p \cdot \mathbb{Z}$. Vamos provar que $J$ é um ideal maximal em $\mathbb{Z}$. De fato, seja $I$ um ideal de $\mathbb{Z}$ tal que,

$$J \subset I \subset \mathbb{Z}.$$

Pelo Teorema 2 do parágrafo 3 temos que existem inteiros $n$ tal que $I = n \cdot \mathbb{Z}$.

Assim, $p \in p \cdot \mathbb{Z} \subset n\mathbb{Z}$, e daí segue $p = n \cdot k$ para algum $k \in \mathbb{Z}$, e portanto $n \backslash p$ e teremos $n = \pm 1$ ou $n = \pm p$.

Se $n = \pm 1$ vem $I = \mathbb{Z}$ e se $n = \pm p$ vem $I = J$ como queríamos demonstrar.

(ii) $\Rightarrow$ (i). Suponhamos $J = p\mathbb{Z}$ um ideal maximal em $\mathbb{Z}$, e seja $d$ um divisor de $p$, isto é, $p = d \cdot b$ onde $b \in \mathbb{Z}$. Vamos provar que $d = \pm 1$ ou $d = \pm p$.

Como $J = p\mathbb{Z} \neq \mathbb{Z}$ segue que $p \neq \pm 1$.

Agora, seja $p = d \cdot b$, então é claro que se $I = d \cdot \mathbb{Z}$ teremos $p \in I$ e $J \subset I \subset \mathbb{Z}$.

Como $J$ é maximal, por hipótese, segue que:

$$J = p \cdot \mathbb{Z} = d \cdot \mathbb{Z} = I \quad \text{ou} \quad I = d \cdot \mathbb{Z} = \mathbb{Z}.$$

Na primeira possibilidade $d \in p\mathbb{Z}$, ou seja $d = p \cdot a$, e daí segue que $p = p \cdot a \cdot b$, e como $p \neq 0$ segue $a \cdot b = 1, a, b, \in \mathbb{Z}$. Assim, teremos que $a = \pm 1$, $b = \pm 1$, e isto finalmente nos diz que $d = \pm p$.

Na segunda possibilidade $d\mathbb{Z} = \mathbb{Z}$ segue imediatamente que $d = \pm 1$. Assim acabamos de provar que os únicos divisores de $p$ são $\pm 1$ e $\pm p$, isto é, $p$ é um número primo. ∎

## §5 Fatorização única

Antes de enunciarmos o teorema principal deste parágrafo, vamos fazer uma observação.

Seja $n \in \mathbb{Z}$, $u \in \{-1, 1\}$ e $p_1, \ldots, p_k$ números primos positivos. Vamos usar a expressão $n = u \cdot p_1 \ldots p_k$ de tal modo que incluiremos na mesma a possibilidade $n = \pm 1$ no caso de $k = 0$, e $n = \pm p_1$ no caso de $k = 1$.

TEOREMA 5 ($\mathbb{Z}$ é um Domínio Fatorial). *Todo número inteiro não nulo n pode ser escrito na forma,*

$$n = u \cdot p_1 \ldots p_k \text{ onde } u \in \{-1, 1\} \text{ e } p_1 \leq p_2 \leq \ldots \leq p_k$$

*são números primos positivos (não necessariamente distintos). Mais ainda, essa expressão é única.*

*Demonstração.* Claramente é suficiente provarmos o teorema para $n \in \mathbb{N} - \{0\} = \{1, 2, \ldots, m, \ldots\}$ e nesse caso $u = 1$ e a expressão se reduz a

$$n = p_1 \cdot p_2 \cdots p_k, p_1 \leq p_2 \leq \ldots \leq p_k \text{ primos} > 0.$$

Vamos primeiramente provar que $n$ pode ser escrito como acima, e a demonstração será por indução sobre $n$.

Se $n = 1$ temos que $n = u \cdot p_1 \ldots p_k$, $u = 1$ e $k = 0$.

Vamos agora supor que todo número inteiro $m$, $1 \leq m < n$ pode ser escrito como produto de primos. Vamos provar que $n$ também pode ser escrito como produto de primos.

Suponhamos, por absurdo, que $n$ não pode ser escrito como produto de primos. Então $n$ não é um número primo, e assim existem divisores $d$ e $d'$ de $n$ tais que: $n = d \cdot d'$, $1 < d$, $d' < n$.

Pela hipótese de indução segue que, $d = q_1 \cdot q_2 \ldots q_r$, $q_1 \leq q_2 \leq \ldots \leq q_r$ são primos positivos, $d' = q'_1 \cdot q'_2 \ldots q'_s$, $q'_1 \leq q'_2 \leq \ldots q'_s$ são primos positivos.

Daí segue,

$$n = d \cdot d' = (q_1 \cdots q_r) \cdot (q'_1 \cdots q'_s)$$

e rearranjando os números primos $q_1, \ldots, q_r, q'_1, \ldots, q'_s$ podemos escrever,

$$n = p_1 \cdot p_2 \cdots p_k \quad \text{onde} \quad k = r + s$$

e $p_1 \leq p_2 \leq \ldots \leq p_k$ como queríamos demonstrar.

Vamos agora demonstrar a unicidade da expressão $n = u \cdot p_1 \ldots p_k$, $u \in \{-1, 1\}$ e $p_1 \leq \ldots \leq p_k$ primos $> 0$.

De fato, seja $n = u \cdot p_1 \ldots p_k$, $p_1 \leq p_2 \leq \ldots \leq p_k$ primos positivos e $n = u' \cdot p'_1 \ldots p'_s$, $p'_1 \leq p'_2 \leq \ldots \leq p'_s$ primos positivos.

Assim,

$$u \cdot p_1 \ldots p_k = u' \cdot p' \ldots p'_s \Rightarrow u = u'$$

e

$$p_1 \ldots p_k = p'_1 \ldots p'_s.$$

Vamos agora provar que isto implica que $k = s$ e $p_i = p'_i$, $i = 1, 2, \ldots, k$.

A demonstração será por indução sobre o inteiro $k$.

Seja $k = 1$. Nesse caso teremos $p_1 = p'_1 \ldots p'_s$ e isso nos diz que $p'_i \backslash p_1$ e como são primos positivos segue que $p_1 = p'_1$ e portanto $s = 1 = k$ e $p_1 = p'_1$.

Suponhamos agora verdadeira a unicidade toda vez que tivermos um produto de $r$ fatores primos positivos onde $1 \leq r < k$ e vamos provar a unicidade para $k$ fatores primos positivos.

Temos, $p_1 \cdot p_2 \ldots p_k = p'_1 \cdot p'_2 \ldots p'_s$, $k \geq 2$. Pela Proposição 5 do parágrafo anterior segue que $\exists\, j$, $1 \leq j \leq s$ tal que $p_1 \backslash p'_j$, e como são primos positivos segue que $p_1 = p'_j$ para algum $j$, $1 \leq j \leq s$. De modo análogo $p'_1 = p_i$ para algum $i$, $1 \leq i \leq k$.

Agora como $p_1 \leq p_2 \leq \ldots \leq p_k$ e $p'_1 \leq p'_2 \leq \ldots \leq p'_s$ segue que $p_1 = p'_1$.

Então teremos, $p_2 \ldots p_k = p'_2 \ldots p'_s$ e daí segue pela hipótese de indução ($r = k - 1$) que: $k - 1 = s - 1$ e $p_2 = p'_2, \ldots, p_k = p'_k$, e assim concluimos que $k = s$ e mais $p_i = p'_i$, $i = 1, 2, \ldots, k$, como queríamos demonstrar.

É conveniente reunirmos os fatores primos iguais na expressão de um inteiro como produto de primos.

Assim, se $n > 1$, $n = p_1 \ldots p_k$, podemos reescrever a expressão acima e obtemos

$$n = q_1^{m_1} \cdot q_2^{m_2} \ldots q_r^{m_r} \quad \text{onde} \quad q_1 \leq q_2 \leq \ldots \leq q_r$$

são os fatores primos distintos de $n$, e pelo Teorema 1 os números inteiros positivos $m_1, \ldots, m_r$ são univocamente determinados pelo inteiro $n$. ■

PROPOSIÇÃO 6. *O conjunto de números primos é infinito.*

*Demonstração.* É suficiente provarmos que o conjunto de números primos positivos é infinito.

Suponhamos, por absurdo, que existem um número finito, $p_1, \ldots, p_n$ de primos positivos.

Se $m = p_1 \ldots p_n + 1$, existe pelo teorema 1, um primo $p$ tal que divide $m$. Se $p = p_i$ para algum $i$, então $p$ divide 1, contradição. ■

Seja $n = p_1^{m_1} \ldots p_r^{m_r}$ onde $p_1, \ldots, p_r$ são os primos divisores distintos de $m$, e cada $m_i > 0$, $i = 1, \ldots, r$. Se $d > 1$ é um divisor de $n$, então é claro que os fatores primos de $d$ pertencem ao conjunto $\{p_1, \ldots, p_r\}$. Assim, convencionado $x^0 = 1$ para $x$ inteiro não nulo, podemos concluir que $d$ pode ser escrito na forma

$$d = p_1^{m'_1} \cdot p_2^{m'_2} \ldots p_r^{m'_r}, \quad \text{onde} \quad 0 \leq m'_i \leq m_i,$$

$i = 1, \ldots, r$.

Desses argumentos acima podemos concluir imediatamente a seguinte proposição:

PROPOSIÇÃO 7. *O número de divisores de um número inteiro não nulo é finito.* ■

EXERCÍCIOS

1. Sejam $m = q_1^{a_1} \dots q_t^{a_t}$ e $n = q_1^{b_1} \dots q_t^{b_t}$ onde $q_1, \dots, q_t$ são números primos e $a_1, \dots, a_t, b_1, \dots, b_t$ são inteiros $\geq 0$.
   Prove que M.D.C. $\{m, n\} = q_{q1}^{c_1} \dots q_t^{c_t}$ onde $C_i = \min\{a_i, b_i\}$.
2. Sejam $J_1, J_2, \dots, J_n, \dots$ ideais de $\mathbb{Z}$. Prove que:
   $J_1 \subset J_2 \subset \dots \subset J_n \subset \dots \Rightarrow \exists\ m \in \mathbb{N}$ tal que $J_k = J_m \ \forall\, k \geq m$.
3. Se $J_i = 2^i \cdot \mathbb{Z}$ Mostre que:
   $$\mathbb{Z} = J_0 \underset{\neq}{\supset} J_1 \underset{\neq}{\supset} J_2 \underset{\neq}{\supset} \dots \underset{\neq}{\supset} J_n \underset{\neq}{\supset} \dots$$
4. Generalize o exercício 3 para primos $p > 2$.

## §6 Os anéis $\mathbb{Z}_n$

Se $J = n \cdot \mathbb{Z}$, a relação $\equiv \pmod n$ pode também ser definida por,

$$x, x' \in \mathbb{Z},\ x \equiv x' \pmod n \Leftrightarrow x - x' \in J$$

e nesse caso usaremos a notação $\bar{x} = x + J = \{x + kn : k \in \mathbb{Z}\}$ para classe de equivalência de $x$ em relação a $\equiv \pmod n$. Usaremos também $\mathbb{Z}_n$, $\mathbb{Z}/_J$ ou $\mathbb{Z}/_{n\cdot\mathbb{Z}}$ para simbolizar o conjunto quociente de $\mathbb{Z}$ pela relação $\equiv \pmod n$.

PROPOSIÇÃO 8. *Se $n \in \mathbb{N} - \{0\}$ então $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ é um conjunto contendo exatamente n classes de equivalência.*

*Demonstração.* Primeiramente vamos provar que se

$$0 \leq x < y < n \text{ então } \bar{x} \neq \bar{y}.$$

De fato, seja $0 \leq x < y < n$. Pela Proposição 1 do parágrafo 3 do capítulo 1, temos que $\bar{y} = \bar{x} \Leftrightarrow y \equiv x \pmod n \Leftrightarrow 0 < y - x = k \cdot n$ para algum $k \in \mathbb{Z}$.

Agora como $0 \leq x < y < n$ temos que $y - x$ não pode ser múltiplo de $n$, ou seja, $\bar{y} \neq \bar{x}$.

Assim $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\} \subset \mathbb{Z}_n$ é um conjunto contendo exatamente $n$ elementos. Para provarmos a igualdade $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ é suficiente mostrarmos que: se $\bar{x} \in \mathbb{Z}_n$ então $\bar{x} \in \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$. Podemos escolher $k$ inteiro positivo suficientemente grande tal que $x' = x + k \cdot n$ seja não negativo. Mas é claro que $x' \equiv x \pmod{n}$, e daí segue que $\bar{x}' = \bar{x}$.

Assim é bastante provarmos que $\bar{x}' \in \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ com $x' \geq 0$. Pelo algoritmo da divisão temos que, $\exists\, q, r \in \mathbb{Z}$ tais que $x' = q \cdot n + r$ onde $0 \leq r < n$.

Mas então $x' - r = qn$ ou $x' \equiv r \pmod{n}$ e portanto $\bar{x} = \bar{x}' = \bar{r}$ e $0 \leq r < n$ como queríamos demonstrar. ■

Observe que se $n = 0$ então $\equiv \pmod{0}$ significa igualdade em $\mathbb{Z}$ e $\mathbb{Z}_n = \{\bar{x} : x \in \mathbb{Z}\}$, é um conjunto infinito. Observe também que $\equiv \pmod{n}$ define a mesma relação que $\equiv \pmod{-n}$.

PROPOSIÇÃO 9. *Seja $n \in \mathbb{N}$. Se $x \equiv x' \pmod{n}$ e $y \equiv y' \pmod{n}$, então:*

(a) $x + y \equiv x' + y' \pmod{n}$
(b) $x \cdot y \equiv x' \cdot y' \pmod{n}$.

*Demonstração.* Por hipótese temos $x - x' = k \cdot n$ e $y - y' = s \cdot n$.

(a) $(x + y) - (x' + y') = (x - x') + (y - y') = (k + s) \cdot n$ e portanto $x + y = x' + y' \pmod{n}$

(b) $x \cdot y = (x' + kn)(y' + s \cdot n) = x'y' + (x's)n + (y'k)n + (ksn)n$.

Portanto,

$$x \cdot y - x' \cdot y' = (x's + y'k + ksn) \cdot n$$

isto é, $x \cdot y \equiv x' \cdot y' \pmod{n}$, como queríamos demonstrar. ■

Como corolário imediato da Proposição 9 segue a seguinte proposição.

PROPOSIÇÃO 10. *Seja $n \in \mathbb{N}$. Se $\bar{x} = \bar{x}'$ e $\bar{y} = \bar{y}'$ então:*

(a) $\overline{x + y} = \overline{x' + y'}$ (a classe da soma independe dos representantes das classes das parcelas)

(*b*) $\overline{x \cdot y} = \overline{x' \cdot y'}$ (a classe do produto independe dos representantes das classes dos fatores).

TEOREMA 6. *Seja n um número inteiro* $\geq 2$.

(a) $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ e $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

$(\bar{x}, \bar{y}) \leadsto \overline{x+y} = \bar{x} + \bar{y}$ $\quad (\bar{x}, \bar{y}) \leadsto \overline{x \cdot y} = \bar{x} \cdot \bar{y}$

definem duas operações (denominadas soma e produto) no conjunto $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.

(b) As operações acima definidas gozam das propriedades de (i) até (viii) enunciadas no parágrafo 1 desse capítulo.

Por isso dizemos que $\mathbb{Z}_n, +, \cdot$ é um *anél comutativo com unidade* $\bar{1}$.

(c) O anel $\mathbb{Z}_n, +, \cdot$ é um domínio de integridade (isto é, sem divisores de zero) $\Leftrightarrow n$ é um número primo.

(d) Se $n = p$ é um número primo então $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ [além das (IX) propriedades enunciadas no parágrafo 1 desse capítulo] goza da seguinte propriedade:

(x) Se $\bar{0} \neq \bar{x} \in \mathbb{Z}_p$ então $\exists\, \bar{y} \in \mathbb{Z}_p$ tal que $\bar{x} \cdot \bar{y} = \bar{y} \cdot \bar{x} = \bar{1}$ [isto é, os elementos diferentes de $\bar{0}$ possuem *inverso multiplicativo*].

*Por isso dizemos que* $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ é *um corpo.*

*Demonstração.* (a) Pela Proposição 10, as regras:

$$\bar{x} + \bar{y} = \overline{x+y} \quad \text{e} \quad \bar{x} \cdot \bar{y} = \overline{x \cdot y}$$

definem operações no conjunto $\mathbb{Z}_n$.

(b) Vamos provar que $\mathbb{Z}_n, +, \cdot$ possui as seguintes 8 propriedades abaixo: sejam $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_n$

(i) associatividade da soma.

$$(\bar{x} + \bar{y}) + \bar{z} = \bar{x} + (\bar{y} + \bar{z})$$

Vamos desenvolver o primeiro membro da igualdade e então chegar no segundo membro, $(\bar{x} + \bar{y}) + \bar{z} = \overline{(x+y)} + \bar{z} = \overline{(x+y)+z}$ e agora pela associatividade da soma em $\mathbb{Z}$ temos que $(\bar{x} + \bar{y}) + \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} + \overline{(y+z)} = \bar{x} + (\bar{y} + \bar{z})$ como queríamos demonstrar.

(ii) Existência do elemento neutro para a soma.

Claramente temos que $\bar{x} + \bar{0} = \bar{0} + \bar{x} = \bar{x}$ e portanto $\bar{0}$ é o elemento neutro para a soma em $\mathbb{Z}_n$.

(iii) Existência de inverso aditivo.

Claramente,

$$\bar{x} + \overline{(-x)} = \overline{(-x)} + \bar{x} = \bar{0}$$

(iv) Comutatividade da soma.

$$\bar{x} + \bar{y} = \overline{x + y} = \overline{y + x} = \bar{y} + \bar{x}$$

(v) Associatividade do produto.

$$(\bar{x} \cdot \bar{y}) \cdot \bar{z} = \overline{(x \cdot y)} \cdot \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \bar{x} \cdot \overline{(y \cdot z)} = \bar{x} \cdot (\bar{y} \cdot \bar{z})$$

(vi) Existência do elemento unidade.
Claramente $\bar{x} \cdot \bar{1} = \bar{1} \cdot \bar{x} = \bar{x}$ e portanto $\mathbb{Z}_n$ possui unidade $\bar{1}$.
(vii) Comutatividade do produto.

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \cdot \bar{x}$$

(viii) Distributividade.

$$\bar{x} \cdot (\bar{y} + \bar{z}) = \bar{x} \cdot \overline{(y + z)} = \overline{x \cdot (y + z)} = \overline{x \cdot y + x \cdot z} =$$
$$= \overline{x \cdot y} + \overline{x \cdot z} = \bar{x} \cdot \bar{y} + \bar{x} \cdot \bar{z}.$$

(c) Vamos provar agora que $\mathbb{Z}_n, +, \cdot$ não possui divisores de zero $\Leftrightarrow n$ é um número primo.

($\Rightarrow$): Suponhamos que $n$ não seja um número primo. Então sabemos que $n = a \cdot b$ onde $1 < a$, $b < n$. Agora $n = a \cdot b$ implica que $\bar{0} = \bar{n} = \bar{a} \cdot \bar{b}$ onde $\bar{a} \neq \bar{0}$ e $\bar{b} \neq \bar{0}$, ou seja, se $n > 2$ não for primo $\mathbb{Z}_n$ possui divisores de zero, ou equivalentemente mostramos a implicação ($\Rightarrow$).

($\Leftarrow$): Suponhamos que $n$ é um número primo, $n = p$, e sejam $\bar{a}, \bar{b} \in \mathbb{Z}_n$.
Se $\bar{a} \cdot \bar{b} = \bar{0}$ vamos provar que $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$ (isto é, $\mathbb{Z}_n$ não possui divisores de zero).

Se $\bar{a} \cdot \bar{b} = \bar{0}$ temos $\overline{a \cdot b} = \bar{0}$, ou seja, $a \cdot b \equiv 0 \pmod{p}$, ou ainda, $p \backslash a \cdot b$ e pela proposição 5 do parágrafo 4 deste capítulo teremos,

$$p \backslash a \quad \text{ou} \quad p \backslash b.$$

Se $p \backslash a$, $\bar{a} = \bar{0}$ e se $p \backslash b$, $\bar{b} = \bar{0}$, como queríamos demonstrar.

(d) Suponhamos que $n = p \geq 2$ é um número primo e seja $\bar{0} \neq \bar{x} \in \mathbb{Z}_p$. Podemos escolher $x$ tal que $0 < x < p$ pois $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$. Ora, $p$ primo e $1 \leq x < p$ implica que M.D.C. $\{x, p\} = 1$ e portanto $\exists\, r, s \in \mathbb{Z}$ tais que $x \cdot r + p \cdot s = 1$ e daí segue (passando a barra) que:

$$\overline{x \cdot r + p \cdot s} = \bar{1}$$

e como $\bar{p} = \bar{0}$ teremos finalmente $\bar{x} \cdot \bar{r} = \bar{1}$, como queríamos demonstrar. ■

Observe que $\mathbb{Q}, +, \cdot$ ; $\mathbb{R}, +, \cdot$ e $\mathbb{C}, +, \cdot$ são exemplos de corpos pois são satisfeitas as propriedades de (i) até (x) para esses anéis, Acabamos de ver que existem também uma infinidade de exemplos de corpos finitos $\mathbb{Z}_p$, $p$ primo $\geq 2$. É claro que todo corpo é um domínio de integridade, ou seja, a propriedade (x) implica na propriedade (ix). Assim todos os exemplos de corpos também são exemplos de domínio de integridade. Finalmente $\mathbb{Z}$ é um exemplo de domínio de integridade que não é corpo e $\mathbb{Z}_n$ quando $n > 2$ não é primo, é um exemplo de anel comutativo com unidade porém com divisores de zero, isto é, não são domínios de integridade.

## EXERCÍCIOS

1. Se $p$ é um número primo $\geq 2$. Prove que $\sqrt{p} \notin \mathbb{Q}$.
2. Seja $\mathbb{Z}[\sqrt{2}] = \{x \in \mathbb{R} : x = a + b\sqrt{2},\ a, b, \in \mathbb{Z}\}$. Defina $+$ e $\cdot$ em $\mathbb{Z}[\sqrt{2}]$ como segue:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = [(a + c) + (b + d)\sqrt{2}]$$
$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = [(ac + 2bd) + (bc + ad)\sqrt{2}]$$

   Prove que: $\forall\, a, b, c, d \in \mathbb{Z}$,
   a) $a + b\sqrt{2} = c + d\sqrt{2} \Leftrightarrow a = c$ e $b = d$.
   b) $\mathbb{Z}[\sqrt{2}], +, \cdot$ satisfaz as propriedades (i), (ii), ..., (ix) e portanto é um domínio de integridade.
   c) Generalize o exercício para $\mathbb{Z}[\sqrt{p}]$, $p$ primo $\geq 2$.

3. Seja $\mathbb{Q}[\sqrt{2}] = \{x \in \mathbb{R} : x = a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$. Defina $+$ e $\cdot$ de modo análogo ao Exercício 2 e prove que: $\forall\, a, b, c, d \in \mathbb{Q}$,
   a) $a + b\sqrt{2} = c + d\sqrt{2} \Leftrightarrow a = c$ e $b = d$.
   b) $\mathbb{Q}[\sqrt{2}], +, \cdot$ satisfaz as propriedades (i), (ii), ..., (ix) e (x) e portanto é um corpo.
   c) Generalize o exercício para $\mathbb{Q}[\sqrt{p}]$, $p$ primo $\geq 2$.
4. Se M.D.C. $\{a, m\} = 1$ prove que:

$$ab \equiv ac \pmod{m} \Rightarrow b \equiv c \pmod{m}$$

5. Se M.D.C. $\{a, m\} = 1$, prove que:
   $\exists$ solução inteira $x$ para a congruência: $ax \equiv b \pmod{m}$.
   Mais ainda, se $x_0$ é uma solução, prove que o conjunto $\mathscr{S}$ de todas as soluções da congruência acima é dado por $\mathscr{S} = x_0 + \mathbb{Z}m = \{x_0 + km : k \in \mathbb{Z}\}$.

6. Ache todos os possíveis inteiros $x$ satisfazendo as seguintes congruências:

a) $3x \equiv 2 \pmod 5$ ; b) $7x \equiv 4 \pmod{10}$
c) $4x + 3 \equiv 4 \pmod 5$ ; d) $6x + 3 \equiv 1 \pmod{10}$
e) $6x + 3 \equiv 4 \pmod{10}$; f) $243x + 17 \equiv 101 \pmod{725}$.

7. Prove que não existe inteiro $x$ satisfazendo a congruência $x^2 \equiv 35 \pmod{100}$.

8. Prove que $\forall\, m \in \mathbb{Z}$ tem-se $m^2 \equiv 0 \pmod 4$ ou $m^2 \equiv 1 \pmod 4$.

9. Achar $x$ inteiro que satisfaz simultaneamente as congruências:

a) $\begin{cases} x \equiv 2 \pmod 5 \\ 3x \equiv 1 \pmod 8 \end{cases}$ ; b) $\begin{cases} 3x \equiv 2 \pmod 5 \\ 2x \equiv 1 \pmod 3 \end{cases}$

10. Sejam $m, n \in \mathbb{N}$ tais que M.D.C. $\{m, n\} = 1$ e sejam $a, b \in \mathbb{Z}$. Mostre que existe inteiro $x$ satisfazendo simultaneamente as congruências:

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n. \end{cases}$$

11. Seja $p$ um primo e $1 \leq n < p$, $n$ inteiro. Mostre que:

$\binom{p}{n} \equiv 0 \pmod p$.

12. Use o Exercício 11 e prove que: se $p$ é um número primo, então:

$$(x + y)^p \equiv x^p + y^p \pmod p \ \forall\, x, y \in \mathbb{Z}.$$

CAPÍTULO III

# ANÉIS, IDEAIS E HOMOMORFISMOS

## §1 Definição e exemplos

Seja $A$ um conjunto não vazio onde estejam definidas duas operações, as quais chamaremos de *soma* e *produto* em $A$ e denotaremos (como em $\mathbb{Z}$) por $+$ e $\cdot$

Assim,

$$\begin{array}{rcl} + : A \times A \to A & \quad \text{e} \quad & \cdot : A \times A \to A \\ (a, b) \rightsquigarrow a + b & & (a, b) \rightsquigarrow a \cdot b \end{array}$$

Chamaremos $A, +, \cdot$ *um anel* se as seguintes 6 propriedades são verificadas quaisquer que sejam $a, b, c \in A$.

A1) $(a + b) + c = a + (b + c)$ (associatividade da soma)

A2) $\exists\ 0 \in A$ tal que $a + 0 = 0 + a = a$ (existência de elemento neutro para a soma)

A3) $\forall\ x \in A$ existe um único $y \in A$, denotado por $y = -x$, tal que $x + y = y + x = 0$ (existência de inverso aditivo).

A4) $a + b = b + a$ (comutatividade da soma)

A5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatividade do produto).

A6) $a \cdot (b + c) = a \cdot b + a \cdot c$; $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributividade à esquerda e à direita).

Se um anel $A, +, \cdot$ satisfaz a propriedade:

A7) $\exists\ 1 \in A$, $0 \neq 1$, tal que $x \cdot 1 = 1 \cdot x = x\ \ \forall x \in A$ dizemos que $A, +, \cdot$ é *um anel com unidade* 1.

Se um anel $A, +, \cdot$ satisfaz a propriedade:

A8) $\forall\ x, y \in A$, $x \cdot y = y \cdot x$, dizemos que $A, +, \cdot$ é *um anel comutativo.*

Se um anel $A, +, \cdot$ satisfaz a propriedade:

A9) $x, y \in A$, $x \cdot y = 0 \Rightarrow x = 0$ ou $y = 0$, dizemos que $A, +, \cdot$ é *um anel sem divisores de zero.*

Se $A, +, \cdot$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $A, +, \cdot$ é *um domínio de Integridade.*

E finalmente, se um domínio de Integridade $A, +, \cdot$ satisfaz a propriedade:

A10) $\forall x \in A, x \neq 0, \exists y \in A$ tal que $x \cdot y = y \cdot x = 1$, dizemos que $A, +, \cdot$ é *um corpo.*

EXEMPLOS de Anéis Comutativos. No capítulo anterior vimos os seguintes exemplos de anéis:

$$\mathbb{Z}, n \cdot \mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[\sqrt{2}], \mathbb{Q}[\sqrt{2}].$$

Observe que todos esses anéis são comutativos e os únicos anéis dessa lista que não possuem unidade são os $n \cdot \mathbb{Z}$, onde $n \geq 2$. Por exemplo, $A = 2 \cdot \mathbb{Z}$ (o anel dos inteiros pares) não possui unidade.

Os únicos anéis que possuem divisores de zero da lista acima são os anéis $A = \mathbb{Z}_n$ onde $n \geq 2$ não é um número primo. Por exemplo, no anel $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ temos que $\bar{2} \cdot \bar{3} = \bar{0}$, isto é, $\bar{2}$ e $\bar{3}$ são divisores de zero em $\mathbb{Z}_6$.

$\mathbb{Z}$ e $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ são exemplos de domínios de Integridade que não são corpos. E finalmente, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Z}_p$, $p$ primo são todos exemplos de corpos, sendo que os $\mathbb{Z}_p$, $p$ primos $\geq 2$, nos dão uma infinidade de exemplos de corpos finitos.

É fácil verificarmos que se substituirmos o 2 por um primo $p \geq 2$ no exemplo $\mathbb{Z}[\sqrt{2}]$ construiremos uma infinidade de exemplos $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Z}\}$ de domínios de integridade que não são corpos.

Analogamente, $\mathbb{Q}[\sqrt{p}]$, $p$ primo $\geq 2$, nos dão uma infinidade de exemplos de corpos $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$ intermediários entre $\mathbb{Q}$ e $\mathbb{R}$. Por exemplo, se $x = a + b\sqrt{p} \neq 0$ em $\mathbb{Q}[\sqrt{p}]$ então $\exists\, y = \dfrac{a - b\sqrt{p}}{a^2 - pb^2}$ tal que $x \cdot y = y \cdot x = 1$.

Se $i = \sqrt{-1} \in \mathbb{C}$ então $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ é um domínio de integridade tal que $\mathbb{Z} \subset \mathbb{Z}[i] \subset \mathbb{C}$. Analogamente, $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ é um corpo tal que $\mathbb{Q} \subset \mathbb{Q}[i] \subset \mathbb{C}$.

Observe também que $\mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\}$ é tal que $\mathbb{C} = \mathbb{R}[i]$.

Em capítulos posteriores, veremos uma infinidade de exemplos de corpos $K$ tais que $\mathbb{Q} \subset K \subset \mathbb{C}$.

Vamos ver agora mais um exemplo de anel comutativo com divisores de zero.

Seja $A = \mathscr{F}(\mathbb{R})$ o conjunto de todas as funções $f: \mathbb{R} \to \mathbb{R}$. Vamos definir duas operações no conjunto $A$ do seguinte modo:

$$+ : \begin{array}{l} A \times A \to A \\ (f, g) \rightsquigarrow f + g \end{array}, \quad \text{onde } (f+g)(x) = f(x) + g(x)\ \forall\, x \in \mathbb{R}$$

$$\cdot : \begin{array}{l} A \times A \to A \\ (f, g) \rightsquigarrow f \cdot g \end{array}, \quad \text{onde } (f \cdot g)(x) = f(x) \cdot g(x)\ \forall\, x \in \mathbb{R}.$$

Observe que a função constante zero é o elemento neutro (em relação a adição) de $A$, e a função constante 1 é o elemento unidade de $A$. As demais propriedades que definem um anel comutativo são claramente verificadas. Assim $A = \mathscr{F}(\mathbb{R}), +, \cdot$ é um anel comutativo com unidade. Porém se $f: \mathbb{R} \to \mathbb{R}$ é definida por

$$f(x) = \begin{cases} 0 & \text{se } x < 0 \\ x & \text{se } x \geq 0 \end{cases}$$

e se $g: \mathbb{R} \to \mathbb{R}$ é definida por

$$g(x) = \begin{cases} x^2 & \text{se } x < 0 \\ 0 & \text{se } x \geq 0 \end{cases}$$

teremos, denotando a função constante zero por $0$, $f \neq 0$, $g \neq 0$ e $f \cdot g = 0$. Assim, o anel $\mathscr{F}(\mathbb{R})$ é um anel comutativo com unidade e com divisores de zero.

Se denotarmos por $\mathscr{C}(\mathbb{R})$ (respectivamente $\mathscr{D}(\mathbb{R})$) o conjunto de todas as funções contínuas (respectivamente deriváveis) $f: \mathbb{R} \to \mathbb{R}$, então de modo análogo ao anterior podemos definir as operações de $+$ e $\cdot$ no conjunto $\mathscr{C}(\mathbb{R})$ (respectivamente $\mathscr{D}(\mathbb{R})$) e também teremos que $\mathscr{C}(\mathbb{R}), +, \cdot$ (respectivamente $\mathscr{D}(\mathbb{R}), +, \cdot$) é uma anel comutativo com unidade e com divisores de zero.

EXEMPLOS de Anéis não Comutativos. Seja $A$ o conjunto de todas as matrizes reais $2 \times 2$, isto é,

$$A = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}.$$

O quadro numérico $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ de números reais diz-se uma *matriz real* $2 \times 2$.

Dizemos que $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \Leftrightarrow \begin{cases} a = a', & b = b' \\ c = c', & d = d' \end{cases}$

Vamos agora definir as operações $+$ e $\cdot$ no conjunto $A$ acima o qual denotaremos por $\text{Mat}_2(\mathbb{R})$.

Sejam $a, b, c, d, a', b', c', d' \in \mathbb{R}$,

soma: $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a+a' & b+b' \\ c+c' & d+d' \end{bmatrix}$

produto: $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{bmatrix}$

Pode-se provar que $\text{Mat}_2(\mathbb{R})$, $+$, $\cdot$ é um anel, onde

$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ é o elemento neutro para a $+$, e $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ é a unidade de $\text{Mat}_2(\mathbb{R})$, $+$, $\cdot$.

Portanto $\text{Mat}_2(\mathbb{R})$ é um anel com unidade.

Observe que se $a \in \mathbb{R}$ e $X_a = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \in \text{Mat}_2(\mathbb{R})$ então $X_a \cdot X_b =$

$= 0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ $\forall\, a, b \in \mathbb{R}$. Assim, o anel $\text{Mat}_2(\mathbb{R})$, $+$, $\cdot$ possui uma infinidade de divisores de zero. Observe também que

$\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$, ou seja, a equação $X^2 = 0$ possui infinitas soluções no anel $\text{Mat}_2(\mathbb{R})$.

Consideremos agora os elementos $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ e $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ de $\text{Mat}_2(\mathbb{R})$ e calculemos,

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

e portanto $\text{Mat}_2(\mathbb{R})$, $+$, $\cdot$ é um exemplo de anel não comutativo, com unidade e com divisores de zero, (generalize esse exemplo para $\text{Mat}_n(\mathbb{R})$, $n > 2$).

Vamos ver agora mais um exemplo de anel não comutativo.

Seja $\mathbb{R}^4 = \{(a, b, c, d) : a, b, c, d \in \mathbb{R}\}$ onde $(a, b, c, d) = (a', b', c', d') \Leftrightarrow a = a'$, $b = b'$, $c = c'$ e $d = d'$.

Vamos definir as operações de soma e produto em $\mathbb{R}^4$.

Sejam $a, b, c, d, a', b', c', d' \in \mathbb{R}$.

soma:

$$(a, b, c, d) + (a', b', c', d') = (a+a',\ b+b',\ c+c',\ d+d')$$

produto:

$$(a, b, c, d)\cdot(a', b', c', d') = (aa' - bb' - cc' - dd', ab' + ba' + cd' - c'd,\ ac' + a'c + db' - d'b,\ ad' + da' + bc' - b'c).$$

Pode-se provar que $\mathbb{R}^4, +, \cdot$ é um anel cujo elemento neutro é $(0, 0, 0, 0)$ e cuja unidade é $(1, 0, 0, 0)$.

É facil verificarmos que:

$$(0, 1, 0, 0)\cdot(0, 0, 1, 0) \neq (0, 0, 1, 0)\cdot(0, 1, 0, 0)$$

e portanto $\mathbb{R}^4, +, \cdot$ é um exemplo de anel não comutativo com unidade.

Vamos agora fazer algumas identificações.

$$\begin{aligned} a &\leftrightarrow (a, 0, 0, 0)\\ i &\leftrightarrow (0, 1, 0, 0)\\ j &\leftrightarrow (0, 0, 1, 0)\\ k &\leftrightarrow (0, 0, 0, 1)\end{aligned}$$

$$a + bi + cj + dk \leftrightarrow (a, b, c, d)$$

Com essas identificações chegamos ao conjunto $\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ onde

$$a + bi + cj + dk = a' + b'i + c'j + d'k \Leftrightarrow a = a', b = b', c = c' e d = d'$$

que será denotado por Quat.

Mais ainda identificando as operações $+$ e $\cdot$ teremos que (verifique)

$$\begin{aligned} i^2 = j^2 &= k^2 = -1\\ i\cdot j = k, &\quad j\cdot i = -k\\ j\cdot k = i, &\quad k\cdot j = -i\\ k\cdot i = j, &\quad i\cdot k = -j\end{aligned}$$

e as operações em Quat são definidas por: sejam $a, b, c, d, a', b', c', d' \in \mathbb{R}$

soma:

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = \\ = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

produto:

Para efetuarmos o produto é suficiente levarmos em conta as regras acima e usarmos a distributividade. Assim,

$$(a + bi + cj + dk) \cdot (a' + b'i + c'j + d'k) =$$
$$= (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i +$$
$$+ (ac' + ca' + db' - bd')j + (ad' + da' + bc' - cb')k.$$

Portanto o anel $\mathbb{R}^4, +, \cdot$ pode ser identificado com o anel Quat, $+, \cdot$. $0 = 0 + 0i + 0j + 0k$ e $1 = 1 + 0i + 0j + 0k$ são, respectivamente, o elemento neutro e a unidade de Quat, $+, \cdot$

Como $i \cdot j \neq j \cdot i$ sabemos que Quat, $+, \cdot$ é um exemplo de um anel não comutativo com unidade. O anel Quat, $+, \cdot$ recebe o nome de *anel dos Quaternios.*

É fácil provar que se

$x = a + bi + cj + dk \neq 0$ então existe um elemento

$y = \dfrac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$ em Quat, $+, \cdot$ tal que, $x \cdot y = y \cdot x = 1$.

Assim, o anel dos quaternios para ser um corpo só falta a propriedade A8) (comutatividade do produto). Por isso, dizemos que Quat, $+, \cdot$ é um *anel de divisão* (ou *um corpo não comutativo*).

Observe que Quat $\supset \mathbb{R}$ e mais ainda, existem 3 cópias do corpo $\mathbb{C}$ dentro do anel Quat, quais sejam,

$$\{a + bi : a, b \in \mathbb{R}\}, \ \{a + cj : a, c \in \mathbb{R}\} \ \text{e} \ \{a + dk : a, d \in \mathbb{R}\}.$$

Como última observação podemos dizer que em Quat, $+, \cdot$ existem infinitas soluções para a equação $X^2 = -1$.

Provaremos mais tarde que, em um corpo, o número de soluções de uma equação polinomial é limitado pelo grau da equação.

## EXERCÍCIOS

1. Prove todas as afirmações feitas nos exemplos do §1.
2. Calcule os divisores de zero nos seguintes anéis:

$$\mathbb{Z}_6, \ \mathbb{Z}_8, \ \mathbb{Z}_{18} \ \text{e} \ \mathbb{Z}_{60}.$$

3. Seja $n$ um inteiro $\geq 2$ e seja $\bar{x} \in \mathbb{Z}_n - \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$, $0 \leq x < n$. Prove que:

$\exists\ \bar{y} \in \mathbb{Z}_n$ tal que $\bar{x} \cdot \bar{y} = \bar{y} \cdot \bar{x} = \bar{1} \Leftrightarrow$ M.D.C. $\{x, n\} = 1$ (isto é, os elementos $\bar{x}, 0 \leq x < n$, invertíveis em $\mathbb{Z}_n$ são aqueles tais que M.D.C. $\{x, n\} = 1$)

4. Seja $f: \mathbb{Z} \to \mathbb{Z}$ uma função tal que $f(x+y) = f(x) + f(y)\ \forall\ x, y \in \mathbb{Z}$ e $f(x \cdot y) = f(x) \cdot f(y)\ \forall x, y \in \mathbb{Z}$. Prove que ou $f = I_{\mathbb{Z}}$ é a função identidade de $\mathbb{Z}$ ou $f = 0$ é a função constante zero.

5. Seja $f: \mathbb{Q} \to \mathbb{Q}$ uma função tal que $f(x+y) = f(x) + f(y)$ e $f(x \cdot y) = f(x) \cdot f(y)\ \forall\ x, y \in \mathbb{Q}$. Prove que ou $f = I_{\mathbb{Q}}$ ou $f = 0$ é a função constante zero.

6. Seja $f: \mathbb{R} \to \mathbb{R}$ uma função tal que, $\forall\ x, y \in \mathbb{R}$, $f(x+y) = f(x) + f(y)$ e $f(x \cdot y) = f(x) \cdot f(y)$. Prove que, se $f$ é contínua então ou $f = I_{\mathbb{R}}$ ou $f = 0$ é a função constante zero.

7. Prove que se $A, +, \cdot$ é um anel qualquer então são válidas as seguintes propriedades quaisquer que sejam $x, y, z \in A$:

a) $0 \cdot x = x \cdot 0 = 0$
b) $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$
c) $(-x) \cdot (-y) = x \cdot y$
d) $x \cdot (y - z) = x \cdot y - x \cdot z$
e) $(y - z) \cdot x = y \cdot x - z \cdot x$

mais ainda se $\exists\ 1 \in A$ então,

f) $(-1) \cdot x = -x$
g) $(-1) \cdot (-1) = 1$
h) $(-1) \cdot (-x) = x$

8. Seja $A, +, \cdot$ um anel qualquer. Vamos definir potência de um elemento $x \in A$ (usando a associatividade do produto) do seguinte modo:

$$x^1 = x, x^2 = x \cdot x, \ldots, x^n = x^{n-1} \cdot x,\ n \geq 2.$$

Prove as seguintes propriedades $\forall\ m, n \in \mathbb{N} - \{0\}$

a) $x^{m+n} = x^m \cdot x^n$
b) $(x \cdot y)^m = x^m \cdot y^m$ se $x \cdot y = y \cdot x$
c) $(x^m)^n = x^{m \cdot n}$
d) Se $xy = yx$ então $(x + y)^n = \sum_{i=1}^{n} \binom{n}{i} \cdot x^i y^{n-i}$

onde $\binom{n}{i} = \dfrac{n!}{(n-i)!\,i!}$.

9. Seja $p$ um número primo $\geq 2$ e seja $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$. Vamos definir uma soma e um produto em $\mathbb{Z}[\sqrt{p}]$ do seguinte modo:

   soma: $(a + b\sqrt{p}) + (c + d\sqrt{p}) = (a + c) + (b + d)\sqrt{p}$, $a$, $b$, $c, d \in \mathbb{Z}$

   produto: $(a + b\sqrt{p}) \cdot (c + d\sqrt{p}) = (ac + pbd) + (bc + ad)\sqrt{p}$, $a, b, c, d \in \mathbb{Z}$. Prove que: $\mathbb{Z}[\sqrt{p}], +, \cdot$ é um domínio de integridade.

10. Seja $p$ um número primo e seja $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$. Defina soma e produto como acima e verifique que $\mathbb{Q}[\sqrt{p}], +, \cdot$ é um corpo.

11. Mostre que o anel $\mathscr{C}[0, 1]$ das funções reais contínuas definidas em $[0, 1]$ possui divisores de zero.

12. Seja $A$ um domínio de integridade e $a, b, c \in A$. Prove que, se $a \neq 0$ e $ab = ac$ então $b = c$.

13. Seja $p$ um número primo $\geq 2$ e seja

$$A = \left\{\frac{m}{n} \in \mathbb{Q} : \text{M.D.C. } \{p, n\} \middle| = 1\right\}.$$

   Mostre que $A$ é um anel com as operações usuais de fração.

14. Seja $D$ um domínio de integridade e seja $a \in D$, $a \neq 0$. Então, prove que a função $\varphi_a : D \to D$ é injetiva.
$$x \rightsquigarrow a \cdot x$$

15. Use o Exercício 14 para provar que todo domínio de integridade finito é um corpo.

16. Seja $A$ um anel tal que $x^2 = x\ \forall\, x \in A$. Prove que $A$ é um anel comutativo.

17. Seja $A$ um anel qualquer e $x \in A$. Se $\exists\, n \in \mathbb{N} - \{0\}$ tal que $x^n = 0$ dizemos que o elemento $x$ é nilpotente.

    (a) Dê exemplos de uma infinidade de elementos nilpotentes em um anel não comutativo.

    (b) Prove que se $x, y \in A$, são elementos nilpotentes de $A$ e $x \cdot y = y \cdot x$ então $x \pm y$ é um elemento nilpotente de $A$.

    (c) Mostre com um exemplo que a hipótese $x \cdot y = y \cdot x$ é essencial em (b).

(d) Seja $x$ um elemento nilpotente em $A$. Mostre que, se $A$ possui unidade $1 \in A$ então o elemento $1 - x$ possui inverso multiplicativo (calcule uma fórmula para esse inverso)

18. Seja $A = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ onde $i^2 = -1$ e

$$a + bi = c + di \Leftrightarrow a = c \text{ e } b = d$$

vamos definir $+$ e $\cdot$ em $A$ do seguinte modo para $a, b, c, d \in \mathbb{Z}$

soma: $(a + bi) + (c + di) = (a + c) + (b + d)i$
produto: $(a + bi) + (c + di) = (ac - bd) + (ad + bc)i$

Prove que $A = \mathbb{Z}[i], +, \cdot$ é um domínio de integridade e calcule todos os elementos de $\mathbb{Z}[i]$ que são invertíveis relativamente ao produto em $\mathbb{Z}[i]$.

19. Seja $A$ um anel, $B$ um conjunto e $f : B \to A$ uma função bijetiva de $B$ sobre $A$. Se para cada $x, y \in B$ definimos

$$x + y = f^{-1}(f(x) + f(y)) \text{ e } x \cdot y = f^{-1}(f(x) \cdot f(y))$$

Então prove que:

(a) $B, +, \cdot$ é um anel
(b) $f(x + y) = f(x) + f(y)$ e $f(x \cdot y) = f(x) \cdot f(y)$ $\forall x, y \in B$.

20. Prove que se definirmos no conjunto $\mathscr{F}(\mathbb{R})$ de todas as funções $f : \mathbb{R} \to \mathbb{R}$ a soma usual de função:
$(f + g)(x) = f(x) + g(x)$ $\forall x \in \mathbb{R}$, e o produto como $(g \cdot f)(x) = g(f(x))$ $\forall x \in \mathbb{R}$, então $\mathscr{F}(\mathbb{R}), +, \cdot$ *não é um anel.*

## §2 Subanéis

Seja $A, +, \cdot$ um anel e $B$ um subconjunto não vazio de $A$. Suponhamos que $B$ seja fechado para as operações $+$ e $\cdot$ de $A$, isto é,

a) $x, y \in B \Rightarrow x + y \in B$
b) $x, y \in B \Rightarrow x \cdot y \in B$.

Assim podemos também considerar a soma e o produto como operações em $B$. Se $B, +, \cdot$ for um anel com as operações de $A$ dizemos que $B$ *é um subanel* de $A$.

Vamos agora dar um critério para que um subconjunto de um anel seja um subanel.

PROPOSIÇÃO 1. *Seja $A, +, \cdot$ um anel e seja $B$ um subconjunto de $A$. Então, $B$ é um subanel de $A$ se e somente se as seguintes condições são verificadas:*

(i) $0 \in B$ (*o elemento neutro de A pertence a B*)

(ii) $x, y \in B \Rightarrow x - y \in B$ (*B é fechado para a diferença*)

(iii) $x, y \in B \Rightarrow x \cdot y \in B$ (*B é fechado para o produto*).

*Demonstração.* ($\Rightarrow$) Se $B$ é um subanel então por definição temos claramente as condições (i), (ii) e (iii).

Observe que o elemento neutro $0'$ de $B$ relativamente a adição é o mesmo elemento neutro $0$ de $A$, pois se $b \in B$, então $0' = b + (-b) = 0$.

($\Leftarrow$) Suponhamos que $B \subset A$ e as três propriedades (i), (ii) e (iii) são satisfeitas.

Por (i) segue que $B \neq \varnothing$, e por (i) e (ii) temos que:

(*) se $x \in B$ então $-x = 0 - x \in B$.

Agora, por (ii) e por (*) teremos, se $x, y \in B$ então $x + y = x - (-y) \in B$, isto é, $B$ é fechado para a soma. Por (iii) $B$ é fechado para o produto.

Como as propriedades associativa, comutativa e distributivas são hereditárias segue imediatamente que $B$ é um subanel de $A$. ■

EXEMPLOS. Se $B$ é subanel de $A$ vamos usar a notação $B \leq A$.

Nos parágrafos anteriores já vimos os seguintes exemplos de subanéis.

a) $n\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \leq$ Quat, onde $n \in \mathbb{N}$

b) $\mathscr{D}(\mathbb{R}) \leq \mathscr{C}(\mathbb{R}) \leq \mathscr{F}(\mathbb{R})$

c) $n\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Z}[\sqrt{p}] \leq \mathbb{Q}[\sqrt{p}] \leq \mathbb{R}$, onde $n \in \mathbb{N}$ e $p$ é um número primo $\geq 2$.

Por exemplo vamos provar que $\mathbb{Z}[\sqrt{p}]$ é um subanel de $\mathbb{R}$.

De fato, $\mathbb{Z}[\sqrt{p}] \subset \mathbb{R}$ e mais:

(i) $0 = 0 + 0\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$

(ii) $x = a + b\sqrt{p},\ y = c + d\sqrt{p} \Rightarrow x - y = (a - c) + (b - d)\sqrt{p}$

(iii) $x = a + b\sqrt{p},\ y = c + d\sqrt{p} \Rightarrow x \cdot y = (ac + pdb) + (bc + ad)\sqrt{p}$ e portanto $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Z}\}$ é um subanel de $\mathbb{R}$.

Se um subanel $B, +, \cdot$ de um corpo $K, +, \cdot$ é também um corpo dizemos que *B é um subcorpo de K*. Observe que $\mathbb{Q}[\sqrt{p}]$ é um subcorpo

de $\mathbb{R}$ enquanto $\mathbb{Q}[i]$ é um subcorpo de $\mathbb{C}$. Observe também que $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ não é um subanel de $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.

O exemplo $2\mathbb{Z} \leq \mathbb{Z}$ nos mostra que um subanel de um anel com unidade não possui necessariamente unidade. Agora vamos ver um exemplo de um subanel $B$ de um anel $A$ tal que a unidade $1'$ de $B$ é diferente da unidade 1 de $A$.

Seja $A = \text{Mat}_2(\mathbb{R})$ e seja $B = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R} \right\}$. Claramente, $B$ é um subanel de $A$.

Vamos agora mostrar que,

$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ é a unidade de $A = \text{Mat}_2(\mathbb{R})$ enquanto

$1' = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ é a unidade de $B$. (observe que $1 \notin B$).

De fato,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \forall\, a, b, c, d \in \mathbb{R}$$

e

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \quad \forall\, a \in \mathbb{R}.$$

Vamos mostrar em seguida que essa patologia não ocorre em anéis sem divisores de zero.

**PROPOSIÇÃO 2.** *As únicas soluções da equação $x^2 = x$ em um domínio de integridade são 0 e 1.*

*Demonstração.* Seja $D$ um domínio de integridade e $x \in D$ tal que $x^2 = x$.

Assim temos,

$$x^2 - x = x \cdot x - 1 \cdot x = (x - 1) \cdot x = 0$$

e daí segue que $x - 1 = 0$ ou $x = 0$, isto é, $x = 1$ ou $x = 0$ como queríamos demonstrar. ■

COROLÁRIO. *Seja D um domínio de integridade com unidade* 1 *e seja B um subanel de D com unidade* 1'.
Então $1 = 1'$.

*Demonstração.* Pela nossa definição de unidade 1 e 1' são diferentes de 0 e como $1^2 = 1$ e $1'^2 = 1'$ o corolário segue imediatamente da Proposição 2. ■

Observe que no anel, $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ (que não é um domínio) temos que:

$$\bar{0}, \bar{1}, \bar{3} \text{ e } \bar{4} \text{ são raízes da equação } x^2 = x.$$

EXERCÍCIOS

1. Seja $\{B_i\}_{i \in \mathbb{N}}$ uma seqüência de subanéis de um anel $A$. Prove que, $B = \bigcap_{i \in \mathbb{N}} B_i$ é também um subanel de $A$.
2. Seja $\{B_i\}_{i \in \mathbb{N}}$ uma seqüência de subanéis de um anel $A$. Prove que, se $B_0 \subset B_1 \subset \ldots \subset B_n \subset \ldots$ então $B = \bigcup_{i \in \mathbb{N}} B_i$ é também um subanel de $A$.
3. Mostre que $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ não é subanel de $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.
4. Seja $A$ um anel e $a \in A$. Prove que, $B = \{x \in A : x \cdot a = a \cdot x\}$ é um subanel de $A$.
5. Seja $A$ um anel. Prove que, $Z(A) = \{x \in A : x \cdot y = y \cdot x \ \forall y \in A\}$ é um subanel (comutativo) de $A$ ($Z(A)$ é chamado *o centro de* $A$)
6. Seja $A$ um anel e $a \in A$. Prove que, $B = \{x \in A : x \cdot a = 0\}$ é um subanel de $A$.
7. Seja $\{K_i\}_{i \in \mathbb{N}}$ uma seqüência de subcorpos de um corpo $K$. Prove que, $B = \bigcap_{i \in \mathbb{N}} K_i$ é um subcorpo de $K$.
8. Seja $\{K_i\}_{i \in \mathbb{N}}$ uma seqüência de subcorpos de um corpo $K$. Prove que, se $K_0 \subset K_1 \subset \ldots \subset K_n \subset \ldots$ então $B = \bigcup_{i \in \mathbb{N}} K_i$ é um subcorpo de $K$.
9. Seja $K$ um corpo e seja $P$ a interseção de todos os subcorpos de $K$. Prove que, $P$ é o menor subcorpo de $K$ ($P$ é chamado de *corpo primo* de $K$).
10. Calcule todos os subanéis de $\mathbb{Z}_{12}$.

11. Um domínio de integridade $D$ é dito de *característica* 0 se $m = 0$ sempre que $ma = 0$ com $a \in D$, $a \neq 0$ e $m \in \mathbb{N}$. $D$ diz-se de *característica finita* se existe $a \in D$, $a \neq 0$, tal que $ma = 0$ para algum inteiro $m \neq 0$. Nesse caso definimos como a *característica* de $D$ o menor inteiro positivo $m$ tal que $ma = 0$ para algum $a \in D$, $a \neq 0$. Prove que,
   (a) se característica de $D$ é $p$ então $p \cdot x = 0 \ \forall x \in D$.
   (b) a característica de $D$ ou é zero ou um número primo.
   (Sugestão para o Exercício 11: $p \cdot x = (p \cdot 1) \cdot x, \ \forall x \in D$)
12. Seja $A, +, \cdot$ um anel com unidade $1 \in A$.

   Vamos definir duas novas operações no conjunto $A$, usando as operações $+$ e $\cdot$ de $A$.

$$a \oplus b = a + b + 1 \quad \forall a, b \in A$$
$$a \odot b = ab + a + b \quad \forall a, b \in A.$$

   Prove que:
   (a) $A, \oplus, \odot$ é um anel.
   (b) Qual é o elemento zero de $A, \oplus, \odot$.
   (c) $A, \oplus, \odot$ possui unidade? Qual?
13. Prove que se $A$ é um anel de divisão então $Z(A)$ é um corpo.
14. Prove que $Z(\text{Quat}) = \mathbb{R}$.

## §3 Ideais e anéis quocientes

Vamos ver agora uma classe de subanéis que são muito importantes na teoria dos anéis, que são os ideais de um anel.

Seja $A$ um anel e seja $I$ um subanel de $A$. Dizemos que $I$ é um *ideal a esquerda* de $A$ se,

(iv) $a \cdot x \in I, \ \forall a \in A, \ \forall x \in I$ (ou simbolicamente $A \cdot I \subset I$).

Analogamente definimos *um ideal à direita* $J$ de um anel $A$ como sendo um subanel de $A$ satisfazendo a condição,

(iv)' $x \cdot a \in J, \ \forall a \in A, \ \forall x \in J$ (ou simbolicamente $J \cdot A \subset J$).

Se $I$ é um ideal simultaneamente à direita e à esquerda de um anel $A$ dizemos que $I$ é *um ideal* de $A$, isto é,

(v) $A \cdot I \subset I$ e $I \cdot A \subset I$.

Se o anel $A$ for comutativo então as condições (iv), (iv)' e (v) são equivalentes e as 3 noções acima coincidem.

Claramente $\{0\}$ e $A$ são ideais de $A$ (ditos *ideais triviais* de $A$). Os ideais não triviais de $A$ são também chamados *ideais próprios* de $A$.

EXEMPLO 1. Seja $A$ o anel $\text{Mat}_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$ e sejam $I$ e $J$ definidos como segue.

$$I = \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} : a, c \in \mathbb{R} \right\} \text{ e } J = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{R} \right\}.$$

Claramente $I$ é um ideal à esquerda de $A$ e $J$ é um ideal à direita de $A$ mas nenhum dos dois é ideal de $A$. Aliás vamos provar agora que os únicos ideais de $A = \text{Mat}_2(\mathbb{R})$ são os triviais (por isso $A$ é chamado de *um anel simples*).

De fato,

Seja $I$ um ideal de $A = \text{Mat}_2(\mathbb{R})$ e vamos assumir que $I \neq \{0\}$. Assim $\exists \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in I$ onde algum dos $a_{ij}$'s é diferente de zero, $1 \leq i, j \leq 2$. Sejam $e_{rs} \in \text{Mat}_2(\mathbb{R})$, $1 \leq r, s \leq 2$ as seguintes matrizes:

$$e_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \; e_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \; e_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \text{ e } e_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Através de cálculos é fácil verificar que $e_{rs} \cdot \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot e_{mn}$ é uma matriz $2 \times 2$ contendo o elemento $a_{sm}$ na posição $(r, n)$ da matriz. Assim como $A \cdot I \subset I$ e $I \cdot A \subset I$ segue que,

$$e_{1s} \cdot \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot e_{m1} = \begin{bmatrix} a_{sm} & 0 \\ 0 & 0 \end{bmatrix} \in I, \text{ onde } 1 \leq s, m \leq 2, \text{ e também,}$$

$$e_{2s} \cdot \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot e_{m2} = \begin{bmatrix} 0 & 0 \\ 0 & a_{sm} \end{bmatrix} \in I \text{ onde } 1 \leq s, m \leq 2.$$

Daí concluimos que $\forall\, s, m$, $1 \leq s, m \leq 2$, temos:

$$\begin{bmatrix} a_{sm} & 0 \\ 0 & a_{sm} \end{bmatrix} = \begin{bmatrix} a_{sm} & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & a_{sm} \end{bmatrix} \in I.$$

Escolhamos $s, m$, $1 \leq s, m \leq 2$ de modo que $a_{sm} \neq 0$. Assim, $\begin{bmatrix} a_{sm}^{-1} & 0 \\ 0 & a_{sm}^{-1} \end{bmatrix} \cdot \begin{bmatrix} a_{sm} & 0 \\ 0 & a_{sm} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in I$, e como $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ é a unidade do anel $A$ segue imediatamente que $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in I$ quaisquer que sejam $a, b, c, d \in \mathbb{R}$, isto é, $I = \text{Mat}_2(\mathbb{R})$. Acabamos de provar então que se $I \neq \{0\}$ é um ideal de $\text{Mat}_2(\mathbb{R})$ então $I = \text{Mat}_2(\mathbb{R})$ como queríamos demonstrar.

Pode-se provar de modo inteiramente análogo que $\text{Mat}_n(K)$ de todas as matrizes $n \times n$ com coeficientes em um corpo $K$ é um anel simples.

EXEMPLO 2. Vamos agora ver um exemplo de ideais no anel $A = \mathscr{C}[0, 1]$, das funções contínuas $f : [0, 1] \to \mathbb{R}$ com as operações usuais de $+$ e $\cdot$ de funções.

Sabemos que $A$ é um anel comutativo com unidade 1 (função constante 1).

Seja $b \in [0, 1]$ e seja $I = \{f \in A : f(b) = 0\}$. Provemos primeiramente que $I$ é um ideal de $A$.

De fato,

(i) $0 \in I$ pois 0 é a função constante zero.

(ii) se $f, g \in I$ então $(f-g) \in I$ pois $(f-g)(b) = f(b) - g(b) = 0$.

(iii) e (iv): Seja $f \in \mathscr{C}[0, 1] = A$ e $g \in I$. Então, $(f \cdot g)(b) = f(b) \cdot g(b) = f(b) \cdot 0 = 0$. Assim $I$ é um ideal de $A$. Vamos provar agora que $I$ é um *ideal maximal* em $A$ (isto é, $I \neq A$ e os únicos ideais de $A$ contendo $I$ são $I$ e $A$).

De fato,

Se $J$ é um ideal de $A$ e $J \supset I$, $J \neq I$ temos que $\exists f \in J$ tal que $f \notin I$. Assim $f(b) = a \neq 0$. Denotando por a a função constante $a$, temos que:

$$h = f - a \in I \quad \text{pois} \quad h(b) = 0$$

e portanto $a = f - h \in J$ pois $f \in J$ e $h \in I \subset J$. Daí segue que a função constante 1 pertence a $J$ já que $a^{-1} \cdot a = 1$ e $a \in J$. Portanto $J = A$ e $I$ maximal em $A$.

Observe que usamos acima o fato de ser $\mathscr{C}[0, 1]$ um anel contendo as funções constantes.

EXEMPLO 3. Seja $A$ um anel e $x_1, x_2, \ldots, x_n \in A$. É de direta verificação que o conjunto (denotado é definido por)

$$A \cdot x_1 + A \cdot x_2 + \ldots + A \cdot x_n = \{a_1 \cdot x_1 + \ldots + a_n \cdot x_n : a_i \in A\}$$

é um ideal à esquerda de $A$, o qual é chamado de ideal à esquerda *gerado por* $x_1, x_2, \ldots, x_n \in A$.

O ideal $I = A \cdot x_1$ é dito *ideal principal* (à esquerda) gerado por $x_1 \in A$. Analogamente pode se definir ideal à direita de $A$ gerado por $x_1, \ldots, x_n \in A$ e também ideal principal (à direita) gerado por $x_1 \in A$.

Claramente se $A$ é um anel comutativo esses ideais são bilaterais, isto é, à esquerda e direita simultaneamente.

Observe que se $A = 2 \cdot \mathbb{Z}$ e $x_1 = 2 \in A$ então o ideal principal $I = A \cdot x_1 = 4 \cdot \mathbb{Z}$ não contém o elemento gerador $x_1$.

É uma imediata conseqüência de considerações anteriores que se $A$ é um anel com unidade então o ideal gerado por $x_1, \ldots, x_n$ é o menor ideal de $A$ contendo os geradores $x_1, \ldots, x_n$.

Agora vamos ver um Teorema caracterizando corpos.

TEOREMA 1. *Seja* $K, +, \cdot$ *um anel comutativo com unidade* $1 \in K$. *Então as seguintes condições são equivalentes*:

(a) $K$ *é um corpo.*

(b) $\{0\}$ *é um ideal maximal em* $K$.

(c) *os únicos ideais de* $K$ *são os triviais.*

*Demonstração.* (a) $\Rightarrow$ (b). Seja $K$ um corpo e seja $J$ um ideal de $K$ tal que $\{0\} \subset J \subset K$. Suponhamos $J \neq \{0\}$. Assim existe $0 \neq a \in J$. Como $K$ é um corpo existe $b \in K$ tal que $b \cdot a = 1$ e portanto $1 \in J$ e daí segue imediatamente que $J = K$ como queríamos demonstrar.

(b) $\Rightarrow$ (c). Segue imediatamente das definições.

(c) $\Rightarrow$ (a). Para $K$ ser um corpo falta apenas a propriedade $A10$, qual seja, $\forall\, a \in K,\ a \neq 0,\ \exists\, b \in K$ tal que $a \cdot b = b \cdot a = 1$.

Seja $0 \neq a \in K$, e $I = K \cdot a$ o ideal principal de $K$ gerado por $a$.

Ora, $a = 1 \cdot a \in I$, nos diz que $I \neq \{0\}$ e assim pela nossa hipótese teremos $I = K$.

Daí segue,

$$1 \in K = K \cdot a \Rightarrow \exists\, b \in K \text{ tal que } b \cdot a = 1$$

e isto demonstra o Teorema 1. ■

Vamos ver agora que a definição de ideal nos permite generalizar a noção de $\equiv$ (mod $n$) em $\mathbb{Z}$. Vimos no parágrafo 3 do Capítulo 2 que se $J = n \cdot \mathbb{Z}$ e $x, x' \in \mathbb{Z}$, então $x \equiv x' \pmod{n} \Leftrightarrow x - x' \in J$ (é também usual se escrever $x \equiv x' \pmod{J}$) define uma relação de equivalência em $\mathbb{Z}$ e depois construimos o anel quociente $\mathbb{Z}/J$ ou $\mathbb{Z}_n$. Agora vamos generalizar essa idéia para um anel qualquer.

Seja $A$ um anel qualquer e seja $J$ um ideal de $A$. Vamos definir a seguinte relação em $A$,

$$\text{se } \; x, x' \in A, \; x \equiv x' \pmod{J} \Leftrightarrow x - x' \in J.$$

Primeiramente, vamos provar que $\equiv \pmod{J}$ define uma relação de equivalência em $A$.

De fato, quaisquer que sejam $x, x', x'' \in A$, temos

(i) $x \equiv x \pmod{J}$ pois $0 = x - x \in J$

(ii) $x \equiv x' \pmod{J} \Rightarrow x' \equiv x \pmod{J}$ pois se $x - x' \in J$ então $x' - x = - (x - x') \in J$.

(iii) $x \equiv x' \pmod{J}$ e $x' \equiv x'' \pmod{J} \Rightarrow x \equiv x'' \pmod{J}$ pois, $x - x' \in J$ e $x' - x'' \in J \Rightarrow x - x'' = (x - x') + (x' - x'') \in J$.

Denotaremos por $\overline{x} = \{y \in A : y \equiv x \pmod{J}\}$ a qual chamaremos de *classe de equivalência* do elemento $x \in A$ relativamente a relação $\equiv \pmod{J}$.

Agora observe que $y \in \overline{x} \Leftrightarrow y - x \in J$, e por isso também denotaremos a classe $\overline{x}$ por $\overline{x} = x + J = \{x + z : z \in J\}$. Chamaremos de *conjunto quociente de A pelo ideal J* ao conjunto $A/J = \{\overline{x} = x + J : x \in A\}$.

Vamos provar agora uma proposição que nos permitirá definir operações $+$ e $\cdot$ no conjunto quociente $A/J$ de modo a torná-lo um anel (veja a Proposição 9, Capítulo 2, parágrafo 6).

PROPOSIÇÃO 3. *Sejam A um anel e J um ideal em A. Se* $\equiv x' \pmod{J}$ *e* $y \equiv y' \pmod{J}$, então:

(a) $x + y \equiv (x' + y') \pmod{J}$ (b) $x \cdot y \equiv x' \cdot y' \pmod{J}$.

*Demonstração.* (a) Basta observar que, $(x + y) - (x' + y') = (x - x') + (y - y') \in J$ pois $x - x' \in J$ e $y - y' \in J$.

(b) Agora seja $x = x' + a$, $a \in J$ e $y = y' + b$, $b \in J$. Então,

$$x \cdot y - x' \cdot y' = (x' + a) \cdot (y' + b) - x' \cdot y' =$$
$$= x' \cdot y' + x' \cdot b + a \cdot y' + a \cdot b - x'y' = x' \cdot b + a \cdot y' + a \cdot b$$

e como $a, b \in J$ é um *ideal* de $A$ segue $x \cdot y - x' \cdot y' \in J$ como queríamos demonstrar. ■

Como corolário imediato da Proposição 1 segue a seguinte proposição.

PROPOSIÇÃO 4. *Sejam A um anel, J um ideal de A.*
Se $\bar{x} = \bar{x'}$ e $\bar{y} = \bar{y'}$ então
(a) $\overline{x + y} = \overline{x' + y'}$
(b) $\overline{x \cdot y} = \overline{x' \cdot y'}$

O item (a) diz que a classe da soma independe dos representantes das classes das parcelas, enquanto o item (b) diz que a classe do produto independe dos representantes das classes dos fatores. ■

TEOREMA 2. *Seja A um anel e J um ideal de A. Se* $\bar{x} = x + J$ e $A/J = \{\bar{x} : x \in A\}$, *então*:

(a) $+ : A/J \times A/J \to A/J$ e $\cdot : A/J \times A/J \to A/J$
$(\bar{x}, \bar{y}) \rightsquigarrow \overline{x + y} = \bar{x} + \bar{y}$ $\quad$ $(\bar{x}, \bar{y}) \rightsquigarrow \overline{x \cdot y} = \bar{x} \cdot \bar{y}$

*definem duas operações (denominadas soma e produto) em A/J.*
(b) $A/J, +, \cdot$ *é um anel (chamado* anel quociente de A por J)
(c) *Se* 1 *é a unidade de A então* $\bar{1}$ *é a unidade de A/J.*
(d) *Se A é comutativo então A/J é comutativo.*

*Demonstração.* (a) Pela Proposição 4 as regras,

$$\bar{x} + \bar{y} = \overline{x + y} \quad \text{e} \quad \bar{x} \cdot \bar{y} = \overline{x \cdot y}$$

definem operações no conjunto $A/J$.

(b) Veja a demonstração do Teorema 1, do parágrafo 6 do Capítulo 2 e demonstre o item (b).

(c) $1 \cdot x = x \cdot 1 = x \ \ \forall x \in A \Rightarrow \bar{1} \cdot \bar{x} = \bar{x} \cdot \bar{1} = \bar{x}, \ \ \forall \bar{x} \in A/J.$

(d) Se $x \cdot y = y \cdot x \ \ \forall x, y \in A$ então, claramente, teremos,

$$\bar{x} \cdot \bar{y} = \bar{y} \cdot \bar{x} \qquad \forall \bar{x}, \bar{y} \in A/J.$$ ■

**TEOREMA 3.** *Seja A um anel comutativo com unidade* $1 \in A$ *e seja* $J$ um ideal de A. Então:
J é ideal maximal de A $\Leftrightarrow$ *A/J é um corpo.*

*Demonstração.* ($\Rightarrow$): Suponhamos $J$ ideal maximal de $A$, e seja $\bar{0} \neq \bar{a} \in \bar{A} = A/J$. Temos que provar que $\exists\, \bar{b} \in \bar{A}$ tal que $\bar{a} \cdot \bar{b} = \bar{1}$. De fato, se $L = A \cdot a$ ideal principal de $A$ gerado por $a$, teremos que: $J + L = \{x + y : x \in J,\ y \in L\}$ é um ideal contendo $J$, e mais $\bar{a} \neq \bar{0} \Leftrightarrow a \notin J$. Como $a = 1 \cdot a \in L \subset J + L$ temos que $J + L$ é um ideal $\supset J$ e mais $J + L \neq J$.
Pela maximalidade de $J$ segue que $A = J + L$e daí vem, $1 \in J + L \Rightarrow$ $\Rightarrow \exists\, u \in J,\ v \in L$ tais que $1 = u + v$.
Mas $v \in L = A \cdot a$ e temos que $v = b \cdot a$ para algum $b \in A$, ou seja,

$$\exists\, b \in A,\ \exists\, u \in J \text{ tais que } 1 = u + b \cdot a.$$

Ora, passando barra em ambos os membros, segue que, $\bar{1} = \overline{u + b \cdot a} = \bar{u} + \overline{b \cdot a} = \bar{0} + \bar{b} \cdot \bar{a}$, isto é, $\bar{b} \cdot \bar{a} = \bar{a} \cdot \bar{b} = \bar{1}$, como queríamos demonstrar.
($\Leftarrow$) Suponhamos que $\bar{A} = A/J$ seja um corpo. Assim

$$\bar{0}, \bar{1} \in \bar{A} \Rightarrow J \neq A.$$

Se $M \neq J$ é um ideal de $A$ e $J \subset M \subset A$, então teremos que existe $a \in M$, $a \notin J$, ou seja, $\bar{a} \neq \bar{0}$, $a \in \bar{A}$. Como $\bar{A}$ é corpo $\exists\, \bar{b} \in \bar{A}$ tal que $\bar{a} \cdot \bar{b} = \bar{1}$; ou ainda,

$$ab \equiv 1 \pmod{J} \Leftrightarrow ab - 1 \in J \Leftrightarrow \exists\, u \in J \text{ tal que}$$

$ab - 1 = u$, e isto nos diz que,

$$1 = ab - u.$$

Como $a \in M$ segue $ab \in M$ e como $u \in J \subset M$ temos também $u \in M$. Logo concluimos que $1 = ab - u \in M$ e imediatamente temos $M = A$ como queríamos demonstrar. ■

Os Anéis $\mathbb{Z}_n = \mathbb{Z}/J$ onde $J = n \cdot \mathbb{Z}$ já foram por nós analisados no parágrafo 6 do capítulo anterior e até agora são os únicos exemplos de anéis quocientes apresentados. No próximo capítulo será de grande importância o estudo dos anéis quocientes do anel de polinômios em uma variável.

## EXERCÍCIOS

1. Mostre que a interseção de ideais de um anel $A$ é também um ideal de $A$.
2. Seja $\{J_n\}_{n \in \mathbb{N}}$ uma sucessão de ideais de um anel $A$. Prove que, se $J_0 \subset J_1 \subset \ldots \subset J_n \subset \ldots$ então $J = \bigcup_{n \in \mathbb{N}} J_n$ é um ideal de $A$.
3. Seja $p$ um número primo e seja $A$ definido por,
$$A = \left\{ \begin{array}{l} m/n : m,\ n \in \mathbb{Z},\ n \neq 0 \\ \qquad \text{e M.D.C.}\ \{p, n\} = 1 \end{array} \right\}$$
   (a) Prove que $A$ é um subanel de $\mathbb{Q}$.
   (b) Prove que $I = \left\{ m/n \in A : p \backslash m \right\}$ é um ideal de $A$.
4. Seja $A$ um anel e $a \in A$. Prove que $I = \{x \in A : x \cdot a = 0\}$ é um ideal à esquerda de $A$.
5. Sejam $I$ e $J$ ideais de um anel $A$. Prove que,
   (a) $I + J = \{x + y : x \in I,\ y \in J\}$ é um ideal de $A$.
   (b) $I \cdot J = \left\{ \sum_{i=1}^{n} x_i \cdot y_i : n \in \mathbb{N},\ x_i \in I,\ y_i \in J \right\}$ é um ideal de $A$.
6. Seja $I$ um ideal à esquerda e $J$ um ideal à direita do anel $A$. Prove então que,
$$I \cdot J \text{ é um ideal de } A.$$
7. Seja $A$ um anel comutativo e seja $N = \{x \in A : x^n = 0$ para algum $n \in \mathbb{N} - \{0\}\}$. Prove que $N$ é um ideal de $A$ ($N$ é chamado *Radical* de $A$). Mais ainda; prove que se $\bar{x} \in A/N$ e $\bar{x}^n = \bar{0}$ para algum inteiro $n \geq 1$ então $\bar{x} = \bar{0}$. (Sugestão: Prove que se $x^n \in N$ para algum $n$ inteiro $\geq 1$ então $x \in N$).
8. Seja $A$ um anel comutativo com unidade $1 \in A$, e seja $P$ um ideal de $A$. Dizemos que $P$ é um *ideal primo* de $A$ se $P \neq A$ e $\forall\, x, y \notin A$, se $x \cdot y \in P$ então $x \in P$ ou $y \in P$.
   Então prove que,
   (a) $P$ é um ideal primo de $A \Leftrightarrow A/P$ é um domínio de integridade.
   (b) Os únicos ideais primos de $\mathbb{Z}$ são $\{0\}$ e os ideais principais $p \cdot \mathbb{Z}$ onde $p$ é um número primo.
   (c) Se $P$ e um ideal maximal de $A$ então $P$ é um ideal primo de $A$.

9. Seja $A = \mathscr{C}[0, 1]$ o anel das funções reais contínuas (com as operações usuais de soma e produto de funções) definidas no intervalo $[0, 1]$.
   Prove que,
   se $M$ é um ideal maximal de $A$ então $\exists\, a \in [0, 1]$ tal que
   $$M = \{f \in A : f(a) = 0\}.$$

## §4 Homomorfismo de anéis

Sejam $A$ e $A'$ dois anéis. Por comodismo vamos denotar as operações desses anéis pelos mesmos símbolos $+$ e $\cdot$, porém denotaremos por $0$ o elemento neutro de $A$ e por $0'$ o elemento neutro de $A'$. Se ambos anéis $A$ $A'$ possuem unidade denotaremos por $1$ a unidade de $A$ e por $1'$ a unidade de $A'$.

Uma função $f: A \to A'$ diz-se um *homomorfismo* de $A$ em $A'$ se satisfaz as seguintes condições:

(i) $f(x + y) = f(x) + f(y) \quad \forall\, x, y \in A$
(ii) $f(x \cdot y) = f(x) \cdot f(y) \quad \forall\, x, y \in A.$

Se $f: A \to A'$ é um homomorfismo bijetivo dizemos que $f$ é um *isomorfismo* de $A$ sobre $A'$.

Dizemos que dois anéis $A$ e $A'$ são *isomorfos* (e escrevemos $A \simeq A'$) se existir um isomorfismo de $A$ sobre $A'$.

Os homomorfismos $f: A \to A$ também são chamados de *endomorfismos* de $A$, e os isomorfismos de $A$ sobre si mesmo são chamados de *automorfismos* de $A$.

Denotaremos por

$$\text{End}(A) = \{f: A \to A : f \text{ endomorfismo}\}$$
$$\text{Aut}(A) = \{f: A \to A : f \text{ automorfismo}\}$$

Vamos agora provar algumas propriedades elementares de homomorfismos.

**PROPOSIÇÃO 5.** *Sejam $A$ e $A'$ anéis e $f: A \to A'$ um homomorfismo. Então,*

(a) $f(0) = 0'$
(b) $f(-a) = -f(a) \ \forall\, a \in A$
(c) *Se $A$ e $A'$ são domínios de integridade então ou $f$ é a função constante zero ou $f(1) = 1'$.*

(d) *Se $A$ e $A'$ são corpos então ou $f$ é a função constante zero ou $f$ é injetiva.*

*Demonstração.* (a) É claro que em um anel a equação $X + X = X$ tem o elemento neutro como única solução e assim temos,

$$0 + 0 = 0 \Rightarrow f(0+0) = f(0) + f(0) = f(0)$$

e portanto $f(0) = 0'$ que é o elemento neutro de $A'$.

(b) Seja $a \in A$. De $a + (-a) = 0$ segue pelo item ($a$) que:

$$f(a) + f(-a) = 0'$$

ou seja,

$$f(-a) = -f(a).$$

(c) De $1.1 = 1$ segue que $f(1)^2 = f(1)$, isto é, $f(1) \cdot (f(1) - 1') = 0'$. Agora, $A'$ domínio de integridade nos diz que ou $f(1) = 0'$ ou $f(1) = 1'$.

Se $f(1) = 0'$ então segue que $f(x) = f(x \cdot 1) = f(x) \cdot f(1) = = f(x) \cdot 0' = 0'$ $\forall x \in A$, ou seja, $f$ é a função constante zero.

(d) Sejam $A$ e $A'$ corpos e suponhamos que $f$ não é a função constante zero. Assim, pelo item anterior sabemos que $f(1) = 1'$. Vamos provar que $f$ é injetiva. De fato, se $x, y \in A$ e $f(x) = f(y)$ teremos, $f(x-y) = 0'$. Suponhamos por absurdo que $x \neq y$, então $x - y \neq 0$ e $A$ corpo nos diz que $\exists\, b \in A$ tal que $b \cdot (x-y) = 1$ e daí segue que $f(b) \cdot f(x-y) = f(b) \cdot 0' = 1'$ que é uma contradição. ■

Vamos agora ver alguns exemplos de homomorfismos.

EXEMPLOS. Sejam $A$ e $A'$ anéis. Claramente a função constante zero, isto é, a função $h: A \to A'$ tal que $h(x) = 0'$ $\forall x \in A$, é um homomorfismo de $A$ em $A'$. É também imediato que $I_A : A \to A$ (a função identidade de $A$) é um automorfismo de $A$.

Se $J$ é um ideal de $A$ e $\bar{A} = A/J$, a projeção canônica $\pi: A \to \bar{A}$ definida por $\pi(x) = \bar{x}$ $\forall x \in A$ é tal que:

$$\pi(x+y) = \overline{x+y} = \bar{x} + \bar{y} = \pi(x) + \pi(y)$$

e

$$\pi(x \cdot y) = \overline{x \cdot y} = \bar{x} \cdot \bar{y} = \pi(x) \cdot \pi(y), \quad \forall\, x, y \in A,$$

ou seja, $\pi$ é um homomorfismo de $A$ sobre $\bar{A} = A/J$.

Observe que pelos Exercícios 3 e 4 do Parágrafo 1 desse capítulo segue imediatamente que,

$$\text{Aut}(\mathbb{Z}) = \{I_{\mathbb{Z}}\} \quad \text{e} \quad \text{Aut}(\mathbb{Q}) = \{I_{\mathbb{Q}}\}.$$

Agora vamos provar que se $D = \mathbb{Z}[\sqrt{p}]$ então Aut $D = \{I_D, \sigma\}$ onde $\sigma : \mathbb{Z}[\sqrt{p}] \to \mathbb{Z}[\sqrt{p}]$ é definida por $\sigma(m + n\sqrt{p}) = m - n\sqrt{p}$ $\forall\, m, n \in \mathbb{Z}$.

Primeiramente, temos que $\sigma(1) = 1$ pois $D = \mathbb{Z}[\sqrt{p}]$ é um domínio, e daí segue imediatamente que $\sigma(m) = m \ \ \forall\, m \in \mathbb{Z}$.

Portanto se $\sigma \in \text{Aut}(D)$ vem,

$$\sigma(m + n\sqrt{p}) = m + n\sigma(\sqrt{p}) \qquad \forall\, m, n \in \mathbb{Z}.$$

Agora, com $(\sqrt{p})^2 = p$ temos $(\sigma(\sqrt{p}))^2 = \sigma(p) = p$ ou seja existem duas possibilidades para $\sigma(\sqrt{p})$ em $D$, $\sigma(\sqrt{p}) = \sqrt{p}$ ou $\sigma(\sqrt{p}) = -\sqrt{p}$. Na primeira obtemos $\sigma = I_D$ e na segunda obtemos $\sigma(m + n\sqrt{p}) = m - n\sqrt{p}$ $\forall\, m, n \in \mathbb{Z}$ como desejávamos mostrar.

Vamos ver a seguir um exemplo que colocaremos sob a forma de proposição.

PROPOSIÇÃO 6. Aut $\mathbb{R} = \{I_{\mathbb{R}}\}$.

*Demonstração.* Seja $\sigma \in$ Aut $\mathbb{R}$. Como $\mathbb{R}$ é um corpo temos que $\sigma(1) = 1$ e daí segue imediatamente que $\sigma(m) = m \ \ \forall\, m \in \mathbb{Z}$. É de fácil verificação que $\sigma(r) = r \ \ \forall\, r \in \mathbb{Q}$. Se soubessemos que $\sigma$ é uma função contínua teríamos, passando ao limite, que $\sigma(x) = x$ $\forall\, x \in \mathbb{R}$.

Primeiramente provaremos que $\sigma$ preserva a ordem em $\mathbb{R}$, isto é, se $a < b$ então $\sigma(a) < \sigma(b)$.

De fato,

Se $a < b$ temos $0 < b - a$ e então $\exists\, \alpha \in \mathbb{R}$ tal que $b - a = \alpha^2 > 0$ e daí segue que $\sigma(b - a) = \sigma(\alpha^2) = \sigma(\alpha)^2 > 0$, ou seja, $0 < \sigma(b) - \sigma(a)$ e isto nos dá $\sigma(a) < \sigma(b)$.

Agora, se $x \in \mathbb{R}$ $\exists$ seqüências de racionais $\{r_n\}_{n\in\mathbb{N}}$ e $\{s_m\}_{m\in\mathbb{N}}$ tais que $r_n < x < s_m$ $\forall\, m, n$ e $x = \lim\limits_{n\to\infty} r_n = \lim\limits_{m\to\infty} s_m$. Assim, teremos

$$r_n = \sigma(r_n) < \sigma(x) < \sigma(s_m) = s_m \qquad \forall\, m, n$$

e isto nos dá $\sigma(x) = \lim\limits_{n\to\infty} r_n = x$ como queríamos demonstrar ∎

Vamos terminar esse parágrafo demonstrando o primeiro teorema de homomorfismo.

TEOREMA 4. *Sejam $A$ e $A'$ anéis e $f : A \to A'$ um homomorfismo. Então,*

(1) $\text{Im } f = \{f(a) : a \in A\}$ *é um subanel de* $A'$.
(2) $N(f) = \{a \in A : f(a) = 0'\}$ *é um ideal de* $A$, *e* $f$ *é injetiva* $\Leftrightarrow N(f) = \{0\}$.
(3) *Os anéis* $A/N(f)$ *e* $\text{Im } f$ *são isomorfos.*

*Demonstração.* (1) De fato, claramente temos:

(i) $0' = f(0) \in Im f$.
(ii) $f(a), f(b) \in Im f \Rightarrow f(a) - f(b) = f(a-b) \in Im f$.
(iii) $f(a), f(b) \in Im f \Rightarrow f(a) \cdot f(b) = f(a \cdot b) \in Im f$.

(2) Vamos provar que $N(f) = \{a \in A : f(a) = 0'\}$ é um ideal de $A$. De fato,

(i) $0 \in N(f)$ pois $f(0) = 0'$.
(ii) $a, b \in N(f) \Rightarrow f(a-b) = f(a) - f(b) = 0' - 0' = 0'$, ou seja, $a - b \in N(f)$.
(iii) seja $x \in A$ e $a \in N(f)$ então

$$f(a \cdot x) = f(a) \cdot f(x) = 0' \cdot f(x) = 0'$$

e

$$f(x \cdot a) = f(x) \cdot f(a) = f(x) \cdot 0' = 0',$$

ou seja, $a \cdot x \in N(f)$ e $x \cdot a \in N(f)$. Assim $N(f)$ é um ideal de $A$.

Agora,
Se $f$ é injetiva, segue imediatamente que $N(f) = \{0\}$ pois $f(0) = 0'$.

Se $f(x) = f(y)$, $x, y \in A$ e $N(f) = \{0\}$ segue, $f(x) - f(y) = 0' \Rightarrow f(x-y) = 0' \Rightarrow x - y \in N(f) = \{0\} \Rightarrow x = y$ e isto demonstra (2).

(3) Vamos definir uma função $F : A/N(f) \to Im f$ bijetiva, a qual provaremos ser também um homomorfismo de anéis.

Defina $F$: $A/N(f) \to \text{Im } f$ por: $F(\bar{x}) = f(x)$.
Observe que $F$ esta "bem definida" e é biunívoca pois:

$$\bar{x} = \bar{y} \Leftrightarrow x \equiv y \pmod{N(f)} \Leftrightarrow x - y \in N(f) \Leftrightarrow$$
$$\Leftrightarrow f(x) - f(y) = 0 \Leftrightarrow F(\bar{x}) = f(x) = f(y) = F(\bar{y}).$$

$$Im(F) = \{F(\bar{x}) : \bar{x} \in A/N(f)\} = \{f(x) : x \in A\} = Im\, f$$

logo $A/N(f) \simeq Im\, f$ como queríamos demonstrar. ■

O subanel $Im\, f$ diz-se *Imagem de* $f$ e o ideal $N(f)$ diz-se *Núcleo de* $f$.

Antes de encerrarmos o parágrafo vamos mostrar que se $A = \mathscr{C}[0, 1]$ e $I = \{f \in A : f(0) = 0\}$ então $A/I \simeq \mathbb{R}$.

De fato, sabemos que $I$ é um ideal máximo em $A$ e portanto pelo teorema 2, $A/I$ é um corpo.

Agora, seja $f \in A$ e $f(0) = a \in \mathbb{R}$. Então $h = f - a \in I$ e teremos $\bar{h} = \overline{f - a} = 0$, ou seja, $\bar{f} = \bar{a}$, onde $a \in \mathbb{R}$.

Evidentemente se $a_1 \neq a_2$ tem-se $\bar{a}_1 \neq \bar{a}_2$ e dessas considerações segue que:

$\mathbb{R} \to A/I$ é um homomorfismo bijetivo, isto é, $\mathbb{R} \simeq A/I$.
$a \rightsquigarrow \bar{a}$

## EXERCÍCIOS

1. Calcule End $(\mathbb{Z}[i])$ e Aut $(\mathbb{Q}[i])$.
2. Prove que os anéis $2\mathbb{Z}$ e $3\mathbb{Z}$ não são isomórfos.
3. Prove que os corpos $\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Q}[\sqrt{3}]$ não são isomórfos.
4. Seja $A$, $+$ um grupo abeliano. Prove que,
   (a) se $f, g \in$ End $(A)$ então $(f + g) \in$ End $(A)$ onde $(f + g)(x) = f(x) + g(x)$ $\forall x \in A$.
   (b) Se $f, g \in$ End $(A)$ então $f \cdot g \in$ End $(A)$ onde $(f \cdot g)(x) = f(g(x))$ $\forall x \in A$.
   (c) End $(A)$, $+$, $\cdot$ é um anel com as operações definidas em $(a)$ e $(b)$.
5. Sejam $A$ e $A'$ anéis. Defina $+$ e $\cdot$ no conjunto $A \times A' = \{(a, a') : a \in A, a' \in A'\}$ de modo que $A \times A'$ seja um anel com essas operações.
6. Se $A \times A'$, $+$, $\cdot$ é o anel definido em 5. Prove que $\pi_1 : A \times A' \to A$, $(a, a') \rightsquigarrow a$ e $\pi_2 : A \times A' \to A'$, $(a, a') \rightsquigarrow a'$ são homomorfismos sobrejetivos. Calcule os núcleos de $\pi_1$ e $\pi_2$.
7. Seja $f : A \to A'$ um homomorfismo e $J'$ um ideal de $A'$. Prove que, $f^{-1}(J') = \{a \in A : f(a) \in J'\}$ é um ideal de $A$.

8. Seja $F : \mathscr{C}[0, 1] \to \mathbb{R}$ definida por $F(f) = f(1/2)$ $\forall f \in \mathscr{C}[0, 1]$.
   (a) Prove que $F$ é um homomorfismo.
   (b) Calcule Im $F$ e $N(F)$.
   (c) Identifique o anel $\mathscr{C}[0, 1]/N(f)$.

9. Seja $A$ um anel com unidade 1. Se $x \in A$ e $n \in \mathbb{Z}$ vamos definir $nx$ do seguinte modo,

$$nx = \begin{cases} 0 \in A \text{ se } n = 0 \in \mathbb{Z} \\ x \text{ se } n = 1 \in \mathbb{Z} \\ x + \ldots + x \; n \text{ vezes se } n \geq 2 \\ (-x) \text{ se } n = -1 \in \mathbb{Z} \\ (-x) + (-x) + \ldots + (-x) \; n \text{ vezes se } n \leq -2. \end{cases}$$

   Prove que:
   (a) $m(x + y) = mx + my$, $\forall\, m \in \mathbb{Z}$, $\forall\, x, y \in A$
   (b) $(mn)1 = (m1) \cdot (n1)$, $\forall\, m, n \in \mathbb{Z}$ e $1 \in A$.

10. Seja $A$ um anel com unidade 1 e seja $\varphi : \mathbb{Z} \to A$ definida por $\varphi(n) = n1$ $\forall\, n \in \mathbb{Z}$.
   (a) Prove que $\varphi$ é um homomorfismo.
   (b) Prove que $\{m \in \mathbb{Z} : m1 = 0 \in A\}$ é um ideal de $\mathbb{Z}$.

11. Seja $D$ um domínio de integridade e seja $\varphi : \mathbb{Z} \to D$ definida por $\varphi(n) = n1$ $\forall\, n \in \mathbb{Z}$. Sabemos que $N(\varphi) = \{m \in \mathbb{Z} : m1 = 0 \in D\}$ é um ideal de $\mathbb{Z}$. Se $N(\varphi) = \{0\}$ dizemos que a *característica do domínio D é zero*.
   Se $N(\varphi) \neq \{0\}$ existe um único inteiro positivo $p$ tal que $N(\varphi) = p\mathbb{Z}$. Nesse caso dizemos que a *característica de D é p*. Prove que $p$ é um número primo tal que $p \cdot x = 0$ $\forall\, x \in D$.

12. Seja $K$ um corpo e seja $P$ a interseção de todos os subcorpos de $K$. Prove que $P$ é o menor subcorpo de $K$ (chamamos $P$ de corpo primo de $K$).

13. Seja $K$ um corpo e seja $P$ o corpo primo de $K$. Prove que,
   (a) se característica de $K = 0$ então $P \simeq \mathbb{Q}$.
   (b) se característica de $K = p$ então $P \simeq \mathbb{Z}_p$.
   (c) Prove que se $K \supset \mathbb{Z}_p$ e $\mathbb{Z}_q$, com $p$, $q$ primos então $p = q$.

14. Seja $A$ um anel com unidade $1 \in A$ e suponhamos que $\exists\, 0 \neq e \in A$ tal que $e^2 = e$ ($e$ diz-se um elemento idempotente de $A$).
   Se $A_1 = A \cdot e = \{a \cdot e : a \in A\}$ e se $A_2 = A \cdot (1 - e) = \{a - ae : a \in A\}$, então prove que:

(1) $A_1$ e $A_2$ são subanéis de $A$ tais que $A_1 \cap A_2 = \{0\}$
(2) $A = A_1 \oplus A_2$ (isto é $\forall\, a \in A\ \exists$ únicos elementos $a_1 \in A_1$ e $a_2 \in A_2$ tais que $a = a_1 + a_2$).

15. Seja $A$ um anel com unidade $1 \in A$ e sejam $e_1, \ldots, e_n \in A - \{0\}$ idempotentes de $A$ tais que $1 = e_1 + \ldots + e_n$, $e_i \cdot e_j = 0$ se $i \neq j$, $1 \leq i, j \leq n$. Prove que, se $A_i = A \cdot e_i = \{a \cdot e_i : a \in A\}$ então $A = A_1 \oplus \ldots \oplus A_n$ (isto é, $\forall\, a \in A\ \exists$ únicos elementos $a_i \in A_i$, $i = 1, \ldots, n$, tais que $a = a_1 + \ldots + a_n$).

## §5 O corpo de frações de um domínio

Neste parágrafo, seguindo a construção do corpo de frações $\mathbb{Q} = \left\{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\right\}$ a partir do domínio $\mathbb{Z}$, vamos construir um corpo $K$ a partir de um dado domínio $D$.

Seja $D$ um domínio de integridade qualquer e seja $D^{\#} = D - \{0\}$. Vamos definir uma relação de equivalência no conjunto, $\mathscr{A} = D \times D^{\#} = \{(a, b) : a \in D,\ b \in D^{\#}\}$. De fato, se $(a, b), (c, d) \in \mathscr{A}$ então $(a, b) \sim (c, d) \Leftrightarrow ad = bc$, claramente define uma relação de equivalência conjunto $\mathscr{A}$.

Vamos denotar por $\frac{a}{b}$ (em vez de $\overline{(a, b)}$) a classe de equivalência

$$\frac{a}{b} = \{(x, y) \in \mathscr{A} : xb = ya\}.$$

Assim,

$$\frac{a}{b} = \frac{x}{y} \text{ em } \mathscr{A}/\sim\ \Leftrightarrow bx = ay \text{ em } D.$$

Agora vamos definir operações $+$ e $\cdot$ no conjunto quociente

$$\mathscr{A}/\sim\ = \left\{\frac{a}{b} : a \in D,\ b \in D^{\#}\right\} = K$$

Sejam $(a, b)$ e $(c, d) \in D \times D^{\#}$. Então,

soma:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

produto:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Observe que se $b, d \in D^{\#}$ então $b \cdot d \in D^{\#}$ pois $D$ é um domínio de integridade.

Como das vezes anteriores em que definimos operações em conjuntos quocientes, vamos provar que as operações acima estão "bem definidas" em $K$.

De fato, suponhamos que $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$ então,

1) $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$

2) $\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$.

De $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$ segue que: $ab' = ba'$ e $cd' = dc'$ em $D$.

Agora, $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} = \frac{a'}{b'} + \frac{c'}{d'} \Leftrightarrow (ad + bc)b'd' = (a'd' + b'c')\, bd$ em $D \Leftrightarrow (ab')(dd') + (cd')(bb') = (a'b)(dd') + (c'd)(bb')$ em $D$ e 1) segue das igualdades $ab' = ba'$ e $cd' = c'd$.

Para a demonstração de 2) basta observar que $\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'} \Leftrightarrow$ $\Leftrightarrow (ab') \cdot (cd') = (a'b)(c'd)$ em $D$ e o resultado segue pelas igualdades $ab' = a'b$ e $cd' = c'd$. Vamos denotar por $a^* = \frac{a}{1}$ onde $a \in D$ e 1 é a unidade de $D$, e denotaremos

$$D^* = \left\{a^* = \frac{a}{1} : a \in D\right\} \subset K = \left\{\frac{a}{b} : a \in D, b \in D^{\#}\right\}.$$

É fácil provar que $D^*$ é um domínio de Integridade com unidade $1^* \in D^*$. Aliás $1^*$ é tal que,

$$\forall \frac{a}{b} \in K \text{ então } \frac{a}{b} \cdot 1^* = 1^* \cdot \frac{a}{b} = \frac{a}{b}$$

e mais ainda, $\forall \frac{a}{b} \in K$ temos $\frac{a}{b} + 0^* = 0^* + \frac{a}{b} = \frac{a}{b}$.

Consideremos agora a seguinte função:

$$\varphi : D \to D^*.$$
$$a \rightsquigarrow a^*,$$

É de imediata verificação que:

a) $\text{Im}\,\varphi = D^*$
b) $N|(\varphi) = \{a \in D : a^* = 0^*\} = \{0\}$
c) $\varphi(a + b) = (a + b)^* = a^* + b^* = \varphi(a) + \varphi(b) \quad \forall\ a, b \in D$
d) $\varphi(a \cdot b) = (a \cdot b)^* = a^* \cdot b^* = \varphi(a) \cdot \varphi(b) \quad \forall\ a, b \in D$

Portanto $D \simeq D^* \subset K$.

Observe também que, se $\frac{a}{b} \neq 0^*$ em $K$, isto é, $a \neq 0$ em $D$, então $\frac{b}{a} \in K$ e mais, $\frac{a}{b} \cdot \frac{b}{a} = 1^*$.

Deixaremos como exercício, a demonstração de que $K, +, \cdot$ é um corpo onde o elemento neutro de $K$ é $0^*$ e a unidade de $K$ é $1^*$.

Como $D \simeq D^* \subset K$ dizemos que $D$ está imerso em $K$. Observe também que $b^* \cdot \frac{1}{b} = 1^*$ se $b \neq 0$, $b \in D$. Assim denotaremos por $(b^*)^{-1} = \frac{1}{b}$ se $b \neq 0, b \in D$. Agora é fácil provar que:

$$D^* = \{a^* : a \in D\} \subset K = \{a^* \cdot (b^*)^{-1} : a^* \in D^*,\ \underset{b^* \neq 0^*}{b^* \in D^*}\}.$$

O corpo $K$ construido nesse parágrafo recebe o nome de *corpo de frações do domínio D*.

Deixaremos ainda como exercício a seguinte proposição.

**PROPOSIÇÃO 7.** *Seja D um domínio de integridade e $D \subset L$ onde L é um corpo. Seja F a interseção de todos os subcorpos de L contendo D (isto é, F é o menor subcorpo de L contendo D). Então, F é isomórfico ao corpo quociente de D.*

(Sugestão: Prove que $F = \{a \cdot b^{-1} : a \in D,\ \underset{b \in D}{b \neq 0}\}$ e depois use $K = \{(a^*) \cdot (b^*)^{-1} : a^* \in D^*,\ \underset{b^* \in D^*}{b^* \neq 0^*}\})$.

CAPÍTULO IV

# POLINÔMIOS EM UMA VARIÁVEL

## §1 Definição e exemplos

Neste capítulo vamos introduzir os polinômios em uma "variável" (ou "indeterminada") e desenvolveremos os parágrafos em completa analogia com o Capítulo 2 (os números inteiros) esperando assim, entre outros objetivos, atingir também uma maior compreensão algébrica de $\mathbb{Z}$.

Seja $K$ um corpo qualquer. Chamamos de *um polinômio sobre K em uma indeterminada x* a uma expressão formal $p(x) = a_0 + a_1x + \ldots + a_mx^m + \ldots$ onde $a_i \in K$, $\forall\, i \in \mathbb{N}$ e $\exists\, n \in \mathbb{N}$ tal que $a_j = 0\ \forall\, j \geq n$.

Dizemos que dois polinômios $p(x) = a_0 + a_1x + \ldots + a_mx^m + \ldots$ e $q(x) = b_0 + b_1x + \ldots + b_kx^k + \ldots$ sobre $K$ são iguais se e somente se $a_i = b_i$ em $K, \forall\, i \in \mathbb{N}$.

Se $p(x) = 0 + 0x + \ldots + 0x^m + \ldots$ indicaremos $p(x)$ por 0 e o chamamos de *o polinômio identicamente nulo sobre K*. Assim um polinômio $p(x) = a_0 + a_1x + \ldots + a_mx^m + \ldots$ sobre $K$ é identicamente nulo $\Leftrightarrow a_i = 0 \in K\ \forall\, i \in \mathbb{N}$.

Se $a \in K$ indicaremos por $a$ ao polinômio $p(x) = a_0 + a_1x + \ldots + a_mx^m + \ldots$ onde $a_0 = a$, e $a_i = 0\ \forall\, i \geq 1$.

Chamamos ao polinômio $p(x) = a$, $a \in K$ de *polinômio constante a*.

Se $p(x) = a_0 + a_1x + \ldots + a_nx^n + \ldots$ é tal que $a_n \neq 0$ e $a_j = 0$ $\forall\, j > n$ dizemos que $n$ é *o grau do polinômio* $p(x)$, e nesse caso indicamos $p(x) = a_0 + a_1x + \ldots + a_nx^n$, e o grau de $p(x)$ por $\partial p(x) = n$.

Vamos denotar por $K[x]$ o conjunto de todos os polinômios, sobre $K$, em uma indeterminada $x$.

Observe que não está definido o grau do polinômio 0, e $\partial$ pode ser interpretada como uma função do conjunto de todos os polinômios $\neq 0$ no conjunto $\mathbb{N}$. Assim,

$$\begin{aligned} \partial : K[x] - \{0\} &\to \mathbb{N} \\ p(x) &\rightsquigarrow \partial p(x) = \text{grau de } p(x) \end{aligned}$$

Agora vamos definir operações soma e produto no conjunto $K[x]$.

Sejam $p(x) = a_0 + a_1x + \ldots + a_ma^m + \ldots$ e $q(x) = b_0 + b_1x + \ldots + b_rx^r + \ldots$ dois elementos do conjunto $K[x]$.

Definimos

$$p(x) + q(x) = c_1 + \ldots + c_k x^k + \ldots \text{ onde } c_i = (a_i + b_i) \in K,$$

e

$$p(x) \cdot q(x) = c_0 + \ldots + c_k x^k + \ldots$$

onde

$$c_0 = a_0 b_0,\ c_1 = a_0 b_1 + a_1 b_0,\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \ldots,$$

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0,\ k \in \mathbb{N}.$$

Observe que a definição acima de produto provém da regra $x^m \cdot x^n = x^{m+n}$ e da propriedade distributiva. Convencionam-se também as regras $x^0 = 1$ e $x^1 = x$.

É de fácil verificação que $K[x], +, \cdot$ é um domínio de Integridade, onde o polinômio 0 é o elemento neutro de $K[x]$ e o polinômio constante 1 é a unidade $K[x]$.

Observe que se identificarmos os elementos $a \in K$ com os polinômios constantes $p(x) = a$ podemos pensar em $K[x]$ contendo o corpo $K$.

Segue imediatamente das definições que a função grau $\partial$ possui as seguintes propriedades:

(i) $\partial(f(x) + g(x)) \leq \max\{\partial f(x), \partial g(x)\}$, quaisquer que sejam os polinômios não nulos $f(x), g(x) \in K[x]$ tais que $f(x) + g(x) \neq 0$.

(ii) $\partial(f(x) \cdot g(x)) = \partial f(x) + \partial g(x)$ quaisquer que sejam os polinômios não nulos $f(x), g(x) \in K[x]$. Suponhamos que um polinômio $p(x) \neq 0$ possua um inverso multiplicativo em $K[x]$. Assim existe $q(x) \neq 0$ em $K[x]$ tal que $p(x) \cdot q(x) = 1$. Pela propriedade (ii) acima segue que $p(x) = a \neq 0$ é um polinômio constante. Portanto, os únicos polinômios invertíveis em $K[x]$ são os polinômios constantes não nulos.

Convém observar que a notação formal de polinômios aqui introduzida é bastante conveniente, porém esconde um pouco o significado preciso do que seja uma indeterminada "$x$". De fato, os polinômios $p(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots$ nada mais são do que uplas $(a_0, a_1, \ldots, \ldots, a_n, \ldots)$ onde $a_i \neq 0$ somente para um número finito de índices e com a canônica definição de igualdade entre uplas. A operação de soma de polinômios corresponde a natural operação de soma de uplas através das suas coordenadas enquanto a operação de produto de polinômios corresponde a seguinte regra de multiplicação

$$(a_0, a_1, \ldots, a_n, \ldots) \cdot (b_0, b_1, \ldots, b_n, \ldots) = (c_0, c_1, \ldots, c_k, \ldots),$$

onde

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0,\ \forall k \in \mathbb{N}.$$

Agora, identificando:

$$1 \leftrightarrow (1, 0, 0, \ldots, 0, \ldots)$$
$$x \leftrightarrow (0, 1, 0, \ldots, 0, \ldots) \qquad e$$

$a_0 + a_1x + \ldots + a_nx^n \leftrightarrow (a_0, a_1, \ldots, a_n, 0, \ldots)$ temos uma realização concreta, através de uplas, das noções de indeterminada "$x$" e de polinômios nessa indeterminada.

Isso nos possibilita melhor entender a diferença entre funções polinomiais (em uma variável) sobre um corpo $K$ e polinômios em uma indeterminada sobre um corpo $K$.

Por uma função polinomial (em uma variável) sobre um corpo $K$ entendemos uma função $f : K \to K$ onde existem $a_0, \ldots, a_n \in K$ tais que $f(u) = a_0 + a_1u + \ldots + a_nu^n, \forall\, u \in K$.

Uma função polinomial $f$ sobre um corpo $K$ é dita *identicamente nula* se $f(u) = 0\ \forall\, u \in K$.

Por exemplo, se $K = \mathbb{Z}_p$, $p$ n.º primo, sabemos que $u^p = u\ \forall\, u \in K$, ou seja a função polinomial $f : \mathbb{Z}_p \to \mathbb{Z}_p$ definida por $f(y) = y^p - y$ é a função identicamente nula sobre $\mathbb{Z}_p$. Mas é claro pela nossa definição de polinômios em uma indeterminada $x$ que $p(x) = x^p - x$ não é o polinômio 0 sobre $\mathbb{Z}_p$. Em termos de uplas esse polinômio seria $(0, -1, 0, \ldots, 0, 1, 0, \ldots)$ onde o 1 figura na $(p + 1)$-ésima coordenada. Assim, dois polinômios distintos podem induzir a mesma função polinomial sobre um corpo $K$. Veremos mais tarde que no caso de corpos infinitos essa patologia não ocorre.

Se $D$ é um domínio de Integridade, então de modo inteiramente análogo à construção de $K[x]$ onde $K$ é um corpo, podemos construir o domínio de integridade $D[x]$ de todos os polinômios na indeterminada "$x$" com coeficientes em $D$. Por exemplo, $\mathbb{Z}[x]$ é o conjunto de todos os polinômios $p(x) = a_0 + \ldots + a_nx^n$, onde $a_i \in \mathbb{Z}$. Esses polinômios serão estudados no próximo capítulo. Um outro exemplo importante que se consegue através dessa construção é o domínio $K[x, y]$ dos polinômios em duas indeterminadas "$x$" e "$y$" com coeficientes em um corpo $K$. De fato, para isso é bastante construir o domínio $D[y]$ em uma indeterminada "$y$" onde $D = K[x]$ é o domínio dos polinômios em uma indeterminada "$x$", com coeficientes em $K$. Observe que pelas nossas considerações anteriores teremos que $x \cdot y = y \cdot x$ em $D[y] = K[x, y]$.

De modo análogo podemos estender nossa construção para os domínios $K[x_1, \ldots, x_n]$ dos polinômios em $n$ indeterminadas $x_1, \ldots, x_n$, com coeficientes em um corpo $K$.

Os respectivos corpos de frações desses domínios serão indicadas com parênteses em lugar de colchetes. Assim,

$$K(x) = \left\{ \frac{f(x)}{g(x)} : \begin{matrix} f(x), g(x) \in K[x] \\ g(x) \neq 0 \end{matrix} \right\}$$

$$D(x) = \left\{ \frac{f(x)}{g(x)} : \begin{matrix} f(x), g(x) \in D[x] \\ g(x) \neq 0 \end{matrix} \right\}$$

$$K(x_1, \ldots, x_n) = \left\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} : \begin{matrix} f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \\ g(x_1, \ldots, x_n) \neq 0 \end{matrix} \right\}$$

Antes de encerrarmos o parágrafo convém observar que certos teoremas que são válidos para $K[x]$, $K$ corpo (como por exemplo o algorítmo da divisão de Euclides) não são válidos em geral para os domínios $D[x]$ onde $D$ é um domínio de Integridade. Pode-se provar por exemplo que os seguintes domínios $K[x, y]$ *e* $\mathbb{Z}[x]$ não são domínios de ideais principais. De fato, o ideal gerado por "$x$" e "$y$" não é principal em $K[x, y]$ e o ideal gerado por "2" e "$x$" não é principal em $\mathbb{Z}[x]$.

Apesar disso alguns resultados importantes se mantém quando passamos de um domínio $D$ para o domínio $D[x]$, como por exemplo, se $D$ é um domínio fatorial então $D[x]$ também o é. Em particular $\mathbb{Z}[x]$ admite fatorização única como produto de certos polinômios que são os análogos dos números primos em $\mathbb{Z}$.

## §2 O algoritmo da divisão

Seja $K$ um corpo e $K[x]$ o domínio dos polinômios sobre $K$ na indeterminada $x$. Vamos agora provar um teorema que diz ser $K[x]$ um domínio Euclidiano.

TEOREMA 1 (Algoritmo da Divisão). *Sejam* $f(x)$, $g(x) \in K[x]$ *e* $g(x) \neq 0$. *Então existem únicos* $q(x)$, $r(x) \in K[x]$ *tais que*:

$$f(x) = q(x) \cdot g(x) + r(x)$$

*onde ou* $r(x) = 0$ *ou* $\partial r(x) < \partial g(x)$.

*Demonstração*. Seja $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ e

$$g(x) = b_0 + b_1 x + \ldots + b_m x^m \ (\partial g(x) = m)$$

Existência:
Se $f(x) = 0$ basta tomar $q(x) = r(x) = 0$. Suponhamos $f(x) \neq 0$. Assim grau $f = n$. Se $n < m$ basta tomar $q(x) = 0$ e $r(x) = f(x)$. Assim podemos assumir $n \geq m$.

Agora seja $f_1(x)$ o polinômio definido por:

$$f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + f_1(x).$$

É fácil observarmos que $\partial f_1 < \partial f$. Vamos demonstrar o teorema por indução sobre $\partial f = n$.

Se $n = 0$, $n \geq m \Rightarrow m = 0$ e portanto $f(x) = a_0 \neq 0$, $g(x) = b_0 \neq 0$ e teremos, $f(x) = a_0 b_0^{-1} g(x)$ e basta tomar $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$.

Pela igualdade $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$ e $\partial f_1(x) < \partial f(x) = n$ temos pela hipótese de indução que: $\exists\, q_1(x), r_1(x)$ tais que:

$$f_1(x) = q_1(x) \cdot g(x) + r_1(x)$$

onde $r_1(x) = 0$ ou $\partial r_1(x) < \partial g(x)$. Daí segue imediatamente que: $f(x) = (q_1(x) + a_n b_m^{-1} x^{n-m}) g(x) + r_1(x)$, e portanto tomando $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r_1(x) = r(x)$ provamos a existência dos polinômios $q(x)$ e $r(x)$ tais que $f(x) = q(x) \cdot g(x) + r(x)$, e $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

Agora vamos provar a unicidade. Sejam $q_1(x)$, $q_2(x)$, $r_1(x)$ e $r_2(x)$ tais que:

$$f(x) = q_1(x) \cdot g(x) + r_1(x) = q_2(x) \cdot g(x) + r_2(x)$$

onde $r_i(x) = 0$ ou $\partial r_i(x) < \partial g(x)$, $i = 1, 2$.
Daí segue: $(q_1(x) - q_2(x)) \cdot g(x) = r_2(x) - r_1(x)$.

Mas se $q_1(x) \neq q_2(x)$ o grau do polinômio do lado esquerdo da igualdade acima é $\geq \partial g(x)$ enquanto que o grau $\partial(r_2(x) - r_1(x)) < \partial g(x)$ o que é uma contradição. Logo $q_1(x) = q_2(x)$ e daí segue $r_1(x) = f(x) - q_1(x) g(x) = f(x) - q_2(x) \cdot g(x) = r_2(x)$ como queríamos demonstrar.■

Se $f(x) = a_0 + a_1 x + \dots + a_n x^n$ é um polinômio não nulo em $K[x]$ e $\alpha \in K$ é tal que $f(\alpha) = a_0 + a_1 \alpha + \dots + a_n \alpha^n = 0 \in K$ dizemos que *$\alpha$ é uma raiz de $f(x)$ em $K$*. Vamos agora provar uma proposição que limita o número dessas raízes em um corpo. Observe que o polinômio $x^2 + 1$ não possui raízes em $\mathbb{R}$.

**PROPOSIÇÃO 1.** *Seja $K$ um corpo e seja $f(x) = a_0 + a_1 x + \dots + a_n x^n$ um polinômio não nulo em $K[x]$ de grau $n$.*

*Então,*

*O número de raízes de $f(x)$ em $K$ é no máximo igual a $\partial f(x) = n$.*

*Demonstração.* Se $f(x)$ não possui raizes em $K$ a proposição está provada.

Suponhamos que $\alpha \in K$ seja uma raiz de $f(x)$.

Como $g(x) = x - \alpha \in K[x]$ podemos usar o algoritmo da divisão. Assim $\exists\, q(x), r(x) \in K[x]$ tais que: $f(x) = q(x) \cdot (x - \alpha) + r(x)$ onde $r(x) = 0$ ou $\partial r(x) < \partial g(x) = 1$. Assim, $r(x) = b_0$ é um polinômio constante, e temos $f(x) = q(x)(x - \alpha) + b_0$ e como $f(\alpha) = 0$ segue que $0 = 0 + b_0$ ou seja $r(x) = 0$ e $f(x) = q(x) \cdot (x - \alpha)$ onde $\partial q(x) = n - 1$.

Agora como não existem divisores de zero em um corpo segue que se $\beta \in K$ é uma raiz qualquer de $f$ então, $f(\beta) = (\beta - \alpha) \cdot q(\beta) = 0 \Rightarrow \beta = \alpha$ ou $\beta$ é também uma raíz de $q(x) \in K[x]$. Assim as raizes de $f$ são $\alpha$ e as raízes de $q(x)$.

Vamos usar indução sobre $\partial f = n$.

Ora se $n = 0$ $f$ não possui raízes em $K$ e nesse caso já vimos que nada há a demonstrar.

Agora por indução, $\partial q(x) < \partial f(x) = n$, $q(x)$ possui no máximo $\partial q(x) = n - 1$ raízes em $K$ e portanto $f(x)$ possui no máximo $n$ raízes em $K$, como queríamos demonstrar. ■

Esta proposição nos dá alguns corolários interessantes.

Seja $K$ um corpo. Se $L \supset K$ é um corpo dizemos que $L$ *é uma extensão* de $K$. Observe que o polinômio $x^2 + 1$ possui duas raízes em $\mathbb{C} \supset \mathbb{R}$.

COROLÁRIO 1. *Seja $f(x) = a_0 + a_1x + \ldots + a_nx^n$ um polinômio não nulo de grau $n$ em $K[x]$. Então, $f(x)$ possui no máximo $n$ raízes em qualquer extensão $L$ de $K$.*

*Demonstração.* Basta observar que se $f(x) \in K[x]$ e $K \subset L$ então $f(x) \in L[x]$ e agora é só usarmos a proposição anterior para o corpo $L$. ■

Observe que o polinômio $x^3 - 2$ não possui raízes em $\mathbb{Q}$, possui apenas uma raiz em $\mathbb{R}$ e possui 3 raízes em $\mathbb{C}$. Assim, ao extendermos o corpo podemos conseguir mais raízes de um dado polinômio, porém esse número de raízes será sempre limitado pelo grau desse mesmo polinômio. Observe também que o fato de estarmos trabalhando com corpos é fundamental em relação ao resultado do corolário 1, para isso recorde que o polinômio $x^2 + 1$ possui infinitas raízes no anel de divisão dos Quatérnios enquanto o polinômio $x^2 + x$ possui 4 raízes no anel $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.

Seja $K$ um corpo e $f(x) = a_0 + a_1x + \dots + a_nx^n$ um polinômio em $K[x]$. Se $u \in K$ denotamos por $f(u)$ a expressão $f(u) = a_0 + a_1u + \dots + a_nu^n \in K$.

Vimos no Parágrafo 1 que sobre $\mathbb{Z}_p = K$ existem diferentes polinômios $f(x) = x^p - x$ e $g(x) = 0$ tais que $f(b) = g(b) = 0\ \forall\, b \in K = \mathbb{Z}_p$. Agora vamos provar que isto não ocorre em corpos infinitos.

COROLÁRIO 2. *Sejam $f(x)$ e $g(x) \in K[x]$ onde $K$ é um corpo com um número infinito de elementos.*
*Então,*

$$f(x) = g(x) \Leftrightarrow f(b) = g(b)\ \forall\, b \in K.$$

*Demonstração.* ($\Rightarrow$) trivial pela definição de igualdade de polinômios.
($\Leftarrow$) seja $h(x) = f(x) - g(x) \in K[x]$. Assim, por hipótese, temos, $h(b) = 0\ \forall\, b \in K$, e como $K$ é infinito segue imediatamente de Proposição 1 que $h(x) = 0$ ou seja $f(x) = g(x)$ como queriamos demonstrar. ∎

Em outras palavras o Corolário 2 acima nos diz que para corpos infinitos é válido o "princípio de identidade" para polinômios.

## EXERCÍCIOS

1. Determine $q(x)$ e $r(x)$ tais que:

$$f(x) = q(x) \cdot g(x) + r(x)$$

onde $r(x) = 0$ ou $\partial r(x) < \partial g(x)$ e $f(x),\ g(x) \in \mathbb{R}[x]$.
(a) $f(x) = x^3 + x - 1$, $g(x) = x^2 + 1$.
(b) $f(x) = x^3 + 1$ , $g(x) = x + 1$.
(c) $f(x) = x^5 - 1$ , $g(x) = x - 1$.
(d) $f(x) = x^4 - 2$ , $g(x) = x^2 - 2$.
(e) $f(x) = x^3 - 2$ , $g(x) = x - \sqrt[3]{2}$.

2. Sejam $f(x), g(x) \in \mathbb{Z}[x]$ e $g(x) = b_0 + b_1x + \dots + b_mx^m$ onde $b_m = 1$. Prove que $\exists\, q(x),\ r(x) \in \mathbb{Z}[x]$ tais que: $f(x) = q(x) \cdot g(x) + r(x)$ onde $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

3. Seja $f(x) \in K[x] - \{0\}$, $K$ um corpo, e seja $L \supset K$ uma extensão de $K$. Prove que, se $\alpha \in L$ é uma raiz de $f(x)$ então $\exists\, q(x) \in L[x]$ tal que $f(x) = (x - \alpha) \cdot q(x)$. [isto é, se $\alpha$ é uma raiz de $f(x)$ em um corpo então $(x - \alpha)$ é um fator de $f(x)$ *nesse corpo*].

4. Seja $K$ um corpo. Dizemos que $K$ é um corpo *algebricamente fechado* se $\forall f(x) \in K[x]\ \exists\, \alpha \in K$ tal que $f(\alpha) = 0$. (Por exemplo $\mathbb{C}$ é um corpo algebricamente fechado).
   Prove que:
   $\mathbb{R}$ não é um corpo algebricamente fechado.
5. Prove que todo polinômio de grau ímpar sobre $\mathbb{R}$ possui uma raiz em $\mathbb{R}$ [Sugestão: use o teorema do valor intermediário].
6. Prove que se $K$ é algebricamente fechado, então todo polinômio $f(x) \in K[x]$ de grau $n \geq 1$ pode ser fatorado em $K$ do seguinte modo:

$$f(x) = c \cdot (x - \alpha_1) \cdot (x - \alpha_2) \ldots (x - \alpha_n)$$

   onde $c \in K$, e $\alpha_1, \ldots, \alpha_n \in K$ são raízes de $f(x)$.
7. Fatore o polinômio $x^4 - 1$ sobre o corpo $K = \mathbb{C}$ como no Exercício 6.
8. Calcule a soma e o produto dos polinômios $f(x) = \bar{2} \cdot x^3 + \bar{4} \cdot x^2 + \bar{3} \cdot x + \bar{3}$ e $g(x) = \bar{3} \cdot x^4 + \bar{2} \cdot x + \bar{4}$ sobre o corpo $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. E sobre o corpo $\mathbb{Z}_7$?
9. Prove que se $D$ é um domínio de Integridade então $D[x]$ é também um domínio de integridade. Conclua daí que se $K$ é um corpo, então $K[x_1, x_2, \ldots, x_n]$ é um domínio de integridade.
10. Se $A$ é um anel comutativo com unidade $1 \in A$ construa o anel $A[x]$ dos polinômios sobre $A$ na indeterminada $x$. Prove que $A[x]$ é também um anel comutativo com unidade.
11. Calcule todas as raizes em $K = \mathbb{Z}_5$ do polinômio $f(x) = x^5 + \bar{3}x^3 + x^2 + \bar{2}x \in \mathbb{Z}[x]$.
12. Seja $K$ um corpo e $L \supset K$ uma extensão de $K$. Se $\alpha \in L$ e $f(x) \in K[x]$, $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ definimos $f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n \in L$.
    (a) Prove que $K[\alpha] = \{f(\alpha) : f(x) \in K[x]\}$ é um domínio de integridade tal que

$$K \subset K[\alpha] \subset L.$$

    (b) Prove que $\psi : K[x] \to K[\alpha]$ é um homomorfismo sobrejetivo.
    $f(x) \rightsquigarrow f(\alpha)$
    (c) $J = \{f(x) \in K[x] : f(\alpha) = 0\}$ é um ideal de $K[x]$
    (d) $K[x]/J \simeq K[\alpha] \subset L$.

13. Prove que $\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}) : f(x) \in \mathbb{Q}[x]\}$ é igual a $\{x + y\sqrt{2} : x, y \in \mathbb{Q}\}$. Prove que o ideal $J = \{f(x) \in \mathbb{Q}[x] : f(\sqrt{2}) = 0\}$ é um ideal maximal de $\mathbb{Q}[x]$ e conclua pelo item (d) do Exercício 12 que $\mathbb{Q}[\sqrt{2}]$ é um corpo (generalize para $\sqrt{p}$, $p$ primo $\geq 2$)

14. Calcule $f(x) \cdot g(x)$, $f(x), g(x) \in K[x]$ nos seguintes casos:
(a) $f(x) = \bar{5}x^3 + \bar{3}x - \bar{4}$; $g(x) = \bar{2}x^2 - x + \bar{3}$ onde $K = \mathbb{Z}_7$.
(b) $f(x) = \bar{7}x^4 - \bar{2}x^2 + \bar{3}$; $g(x) = \bar{3}x^2 + \bar{4}$ onde $K = \mathbb{Z}_{11}$.

15. Calcular uma outra função polinomial $f$ sobre o corpo $K = \mathbb{Z}_5$ que coincida com a função polinomial $x^2 - x + \bar{1}$ sobre $\mathbb{Z}_5$.

16. Mostre que a equação $X^2 = \bar{1}$ possui 4 soluções no anel $\mathbb{Z}_{15}$. Porque?

17. Sejam $D$ e $D'$ dois domínios isomorfos. Prove que: $D[x] \simeq D'[y]$ onde $D[x]$ é o domínio dos polinômios sobre $D$ na indeterminada $x$, e $D'[y]$ é o domínio dos polinômios sobre $D'$ na indeterminada $y$.

18. Prove que: se $F$ é o corpo de frações de um domínio $D$ então,
$$F(x) \simeq D(x),$$
onde $F(x)$ é corpo de frações de $F[x]$ e $D(x)$ é o corpo de frações de $D[x]$.

19. Quantas funções $f : \mathbb{Z}_n \to \mathbb{Z}_n$ existem?

20. Se $K$ é um corpo e $a \in K, a \neq 0$,
(a) Prove que: $\psi : K[x] \to K[x]$, $p(x) \rightsquigarrow p(a \cdot x) = \psi(p(x))$ é um automorfismo de $K[x]$.
(b) O que acontece se $K$ for substituido no item anterior por um domínio $D$? $\psi$ será também automorfismo?

21. Seja $K$ um corpo e $a \in K$.
Prove que:
$$\varphi : K[x] \to K[x]$$
$$p(x) \rightsquigarrow p(x + a) = \varphi(p(x))$$
é um automorfismo de $K[x]$.

22. Seja $K$ um corpo $f(x) \in K[x]$ e $a \in K$. Prove que o resto da divisão de $f(x)$ por $g(x) = x - a$ é $f(a)$.

## §3 Ideais principais e máximo divisor comum

Seja $K$ um corpo. Como sabemos, um ideal principal de $K[x]$ é o conjunto dos múltiplos de um elemento $p(x) \in K[x]$, isto é, tem a forma

$$J = K[x] \cdot p(x) = \{f(x)\ p(x) : f(x) \in K[x]\}$$

Neste parágrafo, vamos provar a existência de Máximo Divisor Comum em $K[x]$ e para isso vamos provar um teorema que diz ser $K[x]$ um domínio principal.

TEOREMA 2. *Todo ideal de* $K[x]$ *é principal.*

*Demonstração.* Seja $J$ um ideal de $K[x]$. Se $J = \{0\}$ então $J$ é gerado por 0. Suponhamos que $J \neq \{0\}$ e escolhemos $0 \neq p(x) \in J$ tal que $\partial p(x)$ seja o menor possível. Se $p(x) = a$ constante $\neq 0$ então $1 = a^{-1} \cdot a \in J$ e assim segue imediatamente que $J = K[x]$ é gerado por $1 \in K[x]$. Suponhamos então $\partial p > 0$.

Como $p(x) \in J$ claramente temos $K[x] \cdot p(x) \subset J$. Agora vamos provar que $J \subset K[x] \cdot p(x)$ e isto demonstra o Teorema 2.

De fato, seja $f(x) \in J$. Pelo algoritmo de Euclides temos que $\exists\, q(x), r(x) \in K[x]$ tais que $f(x) = q(x) \cdot p(x) + r(x)$ onde ou $r(x) = 0$ ou $\partial r(x) < \partial p(x)$.

Agora, como $f(x), p(x) \in J$ segue imediatamente que $r(x) = f(x) - q(x) \cdot p(x) \in J$ e pela minimalidade de nossa escolha do polinômio $p(x) \in J$ segue que $r(x) = 0$ e portanto temos $f(x) = q(x) \cdot p(x) \in K[x] \cdot p(x)$ como queríamos demonstrar. ∎

Antes de enunciarmos o próximo teorema vamos definir a noção de divisibilidade em $K[x]$.

Sejam $f(x), g(x) \in K[x], g(x) \neq 0$. Dizemos $g(x)$ é *um divisor* de $f(x)$ em $K[x]$ (ou $g(x)$ *divide* $f(x)$ em $K[x]$) se $\exists\, h(x) \in K[x]$ tal que,

$$f(x) = h(x) \cdot g(x).$$

Se $g(x)$ é um divisor de $f(x)$ em $K[x]$ escreveremos $g(x) \backslash f(x)$ em $K[x]$.

Se $p_1(x), \ldots, p_m(x) \in K[x]$ sabemos que $J = K[x] \cdot p_1(x) + \ldots + K[x] \cdot p_m(x) = \{f_1(x) \cdot p_1(x) + \ldots + f_m(x) \cdot p_m(x) : f_i(x) \in K[x]\}$

$$i = 1, 2, \ldots, m$$

é o ideal de $K[x]$ gerado por $p_1(x), \ldots, p_m(x) \in K[x]$.

TEOREMA 3 (Existência de M.D.C.). *Sejam*

$$p_1(x), \ldots, p_m(x) \in K[x] - \{0\}$$

*e seja o ideal* $J = K[x] \cdot p_1(x) + \ldots + K[x] \cdot p_m(x)$ *de* $K[x]$ *gerado pelos polinômios não nulos* $p_1(x), \ldots, p_m(x)$.

*Se* $d(x) \in K[x]$ *é tal que* $J = K[x] \cdot d(x)$ *então são válidas as seguintes propriedades:*

(a) $\exists\, r_1(x), \ldots, r_m(x) \in K[x]$ *tais que* $d(x) = r_1(x) \cdot p_1(x) + \ldots + r_m(x) \cdot p_m(x)$.

(b) $d(x)$ *é um divisor comum de* $p_1(x), p_2(x), \ldots, p_m(x)$.

(c) *se* $d'(x)$ *é um divisor comum qualquer de* $p_1(x), p_2(x), \ldots, p_m(x)$ *então* $d'(x)$ *é também um divisor de* $d(x)$.

Um polinômio satisfazendo as condições (b) e (c) chama-se *um M.D.C. de* $p_1(x), \ldots, p_m(x)$ *em* $K[x]$. É claro que se $d(x)$ é um M.D.C. de $p_1(x), \ldots, p_m(x)$ em $K[x]$ $a \in K$, $a \neq 0$ então $a \cdot d(x)$ *é* também um M.D.C. em $K[x]$ desses mesmos polinômios.

*Demonstração.* (a) sai imediatamente da igualdade

$$K[x] \cdot d(x) = K[x] \cdot p_1(x) + \ldots + K[x] \cdot p_m(x).$$

(*b*) *seja* $i \in \{1, \ldots, m\}$ e $K[x] \cdot d(x) = K[x] \cdot p_1(x) + \ldots + K[x] \cdot p_m(x)$. Então é claro que,

$$p_i(x) \in K[x] \cdot p_i(x) \subset K[x] \cdot p_1(x) + \ldots + K[x] \cdot p_m(x) = K[x] d(x)$$

e portanto $\exists\, r_i(x) \in K[x]$ tal que $p_i(x) = r_i(x) \cdot d(x)$, isto é, $d(x)$ é um divisor de cada $p_i(x)$, $i = 1, 2, \ldots, m$.

(c) seja $d'(x)$ um divisor comum em $K[x]$, *de* $p_1(x), \ldots, p_m(x)$, isto é, $\exists\, r_i(x) \in K[x]$ tal que $p_i(x) = r_i(x) \cdot d'(x)$, $i = 1, 2, \ldots, m$.

Assim,

$$K[x] \cdot p_i(x) \subset K[x] \cdot d'(x) \; \forall\, i \in \{1, 2, \ldots, m\}$$

e daí segue que,

$$K[x] \cdot d(x) = K[x] \cdot p_1(x) + \ldots + K[x] \cdot p_m(x) \subset K[x] \cdot d'(x),$$

ou seja, $\exists\, r(x) \in K[x]$ tal que $d(x) = r(x) \cdot d'(x)$ e isto demonstra o Teorema 3. ■

Se $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ é um polinômio não nulo de $K[x]$ tal que $a_n = 1$ dizemos que $f(x)$ é um polinômio *mônico* em $K[x]$. Se $p_1(x), \ldots, p_m(x) \in K[x] - \{0\}$ é claro que existe um único

M.D.C. mônico de $p_1(x), \ldots, p_m(x)$ em $K[x]$. Nesse caso dizemos *o M.D.C. de* $p_1(x), \ldots, p_m(x)$ *em* $K[x]$ o qual denotamos por $\text{M.D.C.}_{K[x]}\{p_1(x), \ldots, p_m(x)\}$. Se $\text{M.D.C.}_{K[x]}\{p_1(x), \ldots, p_m(x)\} = 1$ dizemos que os polinômios são *relativamente primos em* $K[x]$, e nesse caso $\exists\, r_1(x), \ldots, r_m(x) \in K[x]$ tais que $r_1(x) \cdot p_1(x) + \ldots + r_m(x) \cdot p_m(x) = 1$.

EXEMPLO. Vamos provar nesse exemplo que o domínio $A = \mathbb{Z}[x]$ não é um domínio de ideais principais.

De fato, seja $I$ o ideal de $A$ gerado por 2 e $x$, isto é, $I = A \cdot 2 + A \cdot x = \{2p(x) + x \cdot q(x) : p(x),\ q(x) \in \mathbb{Z}[x]\}$.

Suponhamos por absurdo que $A$ é um domínio de ideais principais. Assim existe $d(x) \in A$ tal que $I = A \cdot d(x)$, e isto nos diz que $A \cdot 2 + A \cdot x = A \cdot d(x)$ e portanto $d(x)$ é um M.D.C. de 2 e $x$ em $\mathbb{Z}[x]$. Como 2 é um número primo em $\mathbb{Z}$ e 2 não é divisor de $x$ em $\mathbb{Z}[x]$ pois $1/2 \notin \mathbb{Z}$, segue imediatamente que $d(x) = \pm 1$, ou seja,

$$1 = \text{M.D.C.}\{2, x\} \text{ em } \mathbb{Z}[x] \quad \text{e} \quad A \cdot 2 + A \cdot x = A.$$

Assim existem polinômios $p(x)$ e $q(x)$ com coeficientes inteiros tais que $1 = 2p(x) + x \cdot q(x)$ o que nos dá um absurdo pois o termo independente da expressão $2p(x) + x \cdot q(x)$, $p(x)\ q(x) \in \mathbb{Z}[x]$ é sempre par.

O domínio $A = \mathbb{Z}[x]$ apesar de não ser um domínio de ideais principais é um domínio fatorial e isto nos dá imediatamente a existência de M.D.C. em $\mathbb{Z}[x]$. Apenas o M.D.C. $d(x) \in \mathbb{Z}[x]$ de polinômios $p(x), q(x) \in \mathbb{Z}[x]$ nem sempre pode ser escrito na forma $d(x) = r(x)\,p(x) + s(x)\,q(x)$, com $r(x), s(x) \in \mathbb{Z}[x]$, como acontecia com o M.D.C. em $K[x]$, onde $K$ é um corpo.

EXERCÍCIOS

1. Mostre que $\exists\, p(x), q(x) \in \mathbb{Z}[x]$ tais que $\partial p(x) = \partial q(x) = 2$ e $x^4 + 4 = p(x) \cdot q(x)$.

2. Calcule $\text{M.D.C.}_{\mathbb{C}[x]}\ \{f(x), g(x)\}$ para os seguintes pares de polinômios em $\mathbb{C}[x]$:
   (a) $f(x) = (x-2)^3\,(x-5)^4\,(x-i)$; $g(x) = (x-1)\,(x - 2(x-5)^3$
   (b) $f(x) = (x^2+1)\,(x^2-1)$; $g(x) = (x+i)^3(x^3-1)$.

3. Calcule $\text{M.D.C.}\{f(x), g(x)\}$ para os seguintes pares de polinômios em $\mathbb{Q}[x]$.

(a) $f(x) = x^3 - 6x^2 + x + 4$; $g(x) = x^5 - 6x + 1$
(b) $f(x) = x^2 + 1$; $g(x) = x^6 + x^3 + x + 1$

4. Seja $f(x), g(x) \in K[x] - \{0\}$ e seja $a \in K, a \neq 0$. Então prove que: $d(x)$ é um M.D.C. de $f(x)$ e $g(x)$ em $K[x] \Leftrightarrow a \cdot d(x)$ é um M.D.C. de $f(x)$ e $g(x)$ em $K[x]$.

5. Seja $f(x), g(x) \in K[x] - \{0\}$ e $L \supset K$ uma extensão do corpo $K$. Prove que:
(a) $\underset{K[x]}{\text{M.D.C.}} \{f(x), g(x)\} = \underset{L[x]}{\text{M.D.C.}} \{f(x), g(x)\}$
(b) $f(x)$ e $g(x)$ são relativamente primos em $K[x] \Leftrightarrow f(x)$ e $g(x)$ são relativamente primos em $L[x]$.

6. Defina a noção de M.D.C. em $\mathbb{Z}[X]$ e prove que:

$$\underset{\mathbb{Z}[X]}{\text{M.D.C.}} \{3, x\} = 1.$$

7. Seja $D$ um domínio de integridade. Dizemos que um elemento $u \in D$ é *invertível em* $D$ se $\exists\, v \in D$ tal que $u \cdot v = v \cdot u = 1$. Prove que:
(a) $u, v$ invertíveis em $D \Rightarrow u.v$ invertível em $D$
(b) $u$ invertível em $D \Leftrightarrow u$ divide $x, \forall\, x \in D$.

8. Seja $D = \mathbb{Z}[\sqrt{p}]$ onde $p$ é um número primo. Se $y \in D, y = m + n\sqrt{p}$ defina $N(y) = m^2 - p \cdot n^2$.
(a) Prove que se $y, y' \in D$ então $N(y \cdot y') = N(y) \cdot N(y')$
(b) Prove que se $u$ é invertível em $D$ então $N(u) = \pm 1$.
(c) Calcule os elementos inversíveis de $\mathbb{Z}[\sqrt{2}]$ e $\mathbb{Z}[\sqrt{3}]$.

9. Calcular $q(x)$, $r(x)$ tais que $f(x) = q(x) \cdot g(x) + r(x)$ onde ou $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.
(a) $f(x) = x^5 - x^3 + 3x - 5$; $g(x) = x^2 + 7 \in \mathbb{Q}[x]$.
(b) $f(x) = x^5 - x^3 + 3x - 5$; $g(x) = x - 2 \in \mathbb{Q}[x]$.
(c) $f(x) = x^5 - x^3 + \bar{3}x - \bar{5}$; $g(x) = x + \bar{2} \in \mathbb{Z}_5[x]$.
(d) $f(x) = x^5 - x^3 + \bar{3}x - \bar{5}$; $g(x) = x^3 + x - \bar{1} \in \mathbb{Z}_3[x]$.

10. Quais dos conjuntos $J \subset \mathbb{Q}[x]$ são ideais de $\mathbb{Q}[x]$. Em caso afirmativo, calcule $p(x)$ mônico $\in J$ tal que $J = \mathbb{Q}[x] \cdot p(x)$. Quais $J$ são ideais maximais de $\mathbb{Q}[x]$?
(a) $J = \{f(x) \in \mathbb{Q}[x] : f(1) = f(7) = 0\}$
(b) $J = \{f(x) \in \mathbb{Q}[x] : f(2) = 0; f(5) \neq 0\}$
(c) $J = \{f(x) \in \mathbb{Q}[x] : f(\sqrt{3}) = 0\}$.
(d) $J = \{f(x) \in \mathbb{Q}[x] : f(4) = 0$ e $f(0) = f(1)\}$.

## §4 Polinômios irredutíveis e ideais maximais

Seja $K$ um corpo e $K[x]$ o domínio dos polinômios sobre $K$ na indeterminada $x$.

Nesse parágrafo vamos introduzir os polinômios em $K[x]$ que, dentro da analogia de $K[x]$ com $\mathbb{Z}$, fazem o mesmo papel dos números primos em $\mathbb{Z}$. Esses polinômios serão chamados de polinômios irredutíveis sobre $K$.

Seja $f(x) \in K[x]$ tal que $\partial f(x) \geq 1$. Dizemos que $f(x)$ é um polinômio *irredutível sobre* $K$ se toda vez que $f(x) = g(x) \cdot h(x)$, $g(x)$, $h(x) \in K[x]$ então temos $g(x) = a$ constante em $K$ ou $h(x) = b$ constante em $K$. Se $f(x)$ for não irredutível sobre $K$ dizemos que $f$ é *redutível sobre* $K$.

Claramente temos que todo polinômio de grau 1 sobre um corpo $M$ é irredutível sobre $M$. Observe também que o polinômio $f(x) = x^2 + 1$ é irredutível sobre o corpo $\mathbb{R}$ porém é redutível sobre $\mathbb{C}$. Assim um polinômio $f(x) \in K[x]$ pode ser irredutível sobre $K$ e redutível em uma extensão $L \supset K$.

Agora vamos provar um teorema relacionando polinômios irredutíveis e ideais maximais (veja a comparação com números primos em $\mathbb{Z}$).

**TEOREMA 4.** *Sejam $K$ um corpo e $p(x) \in K[x]$.*
*Então as seguintes condições são equivalentes:*
(a) *$p(x)$ é irredutível sobre $K$.*
(b) *$J = K[x] \cdot p(x)$ é um ideal maximal em $K[x]$.*
(c) *$K[x]/J$ é um corpo, onde $J = K[x] \cdot p(x)$.*

*Demonstração.* A equivalência $(b) \Leftrightarrow (c)$ sai imediatamente do Teorema 3 do Capítulo 3. Assim vamos apenas provar que $(a) \Leftrightarrow (b)$.

$(a) \Rightarrow (b)$: Suponhamos $p(x) \in K[x]$, $p(x)$ irredutível sobre $K$, e seja $J = K[x] \cdot p(x) = \{g(x) \cdot p(x) : g(x) \in K[x]\}$. Como grau $p(x) \geq 1$ temos imediatamente que $J \neq K[x]$.

Se $I = K[x] \cdot h(x)$ é um ideal de $K[x]$ tal que $I \supset J$ vamos provar que $I = J$ ou $I = K[x]$. (Observe que estamos usando o Teorema 2: todo ideal de $K[x]$ é principal).

Assim, $p(x) \in K[x] \cdot p(x) \subset K[x] \cdot h(x)$ nos diz que, $p(x) = g(x) \cdot h(x)$ para algum $g(x) \in K[x]$. Como $p(x)$ é irredutível temos que $g(x) = a \in K - \{0\}$ constante ou $h(x) = b \in K - \{0\}$ constante.

Se $g(x) = a \neq 0$ constante temos que $h(x) = a^{-1} \cdot p(x)$ e portanto $I = K[x] \cdot h(x) \subset K[x] \cdot p(x) = J$ e isto nos dá $I = J$.

Se $h(x) = b \neq 0$ constante temos $I = K[x] \cdot h(x) = K[x]$ e isto termina a implicação $(a) \Rightarrow (c)$.

$(b) \Rightarrow (a)$: Seja $J = K[x] \cdot p(x)$ um ideal máximal em $K[x]$.

Assim $J \neq K[x]$ nos diz que $\partial p(x) \geq 1$.

Suponhamos $g(x), h(x) \in K[x]$ e $p(x) = g(x) \cdot h(x)$. Assim segue imediatamente que $J \subset I = K[x] \cdot h(x)$ e como $J$ é máximal temos que $J = I$ ou $I = K[x]$. Se $J = I$ segue que $h(x) \in J = K[x] \cdot p(x)$ e isto nos diz que $h(x) = f(x) \cdot p(x)$ para algum $f(x) \in K[x]$. Daí segue que $p(x) = g(x) \cdot f(x) \cdot p(x)$. Como $p(x) \neq 0$ e $K[x]$ é um domínio de integridade teremos $1 = g(x) \cdot f(x)$, isto é, $g(x) \in K[x]$ é um polinômio invertível em $K[x]$. Portanto temos imediatamente que $g(x) = a \neq 0$ é um polinômio constante.

Se $I = K[x]$ segue imediatamente que $h(x) = b \neq 0$ constante ou seja $p(x)$ é irredutível sobre $K$ como queríamos demonstrar. ■

Vamos ver aqui alguns exemplos de corpos obtidos através do quociente de domínio do tipo $A = K[x]$, $K$ corpo por um ideal maximal em $A$:

EXEMPLO 1. Primeiramente vamos provar que se $A = \mathbb{R}[x]$ e $I = A \cdot (x^2 + 1)$ então $A/I \simeq \mathbb{C}$. De fato, como $(x^2 + 1)$ é um polinômio irredutível em $K[x]$ segue que $L = A/I$ é um corpo.

Se $p(x) \in A$ então pelo algorítmo da divisão existem polinômios $q(x), r(x) \in A$ tais que:

$p(x) = q(x) \cdot (x^2 + 1) + r(x)$, onde $r(x) = bx + a$ com $a, b \in \mathbb{R}$.

Passando a barra (congruência módulo I) e tendo em vista que $\overline{(x^2 + 1)} = \bar{0}$ temos,

$$\overline{p(x)} = \overline{q(x)} \cdot \overline{(x^2 + 1)} + \overline{r(x)} = \overline{r(x)} = \overline{bx + a} = \bar{b} \cdot \bar{x} + \bar{a}$$

Assim, $L = \{\bar{b} \cdot \bar{x} + \bar{a} : \bar{a}, \bar{b} \in \mathbb{R}\}$. Observe também que se denotarmos $\bar{\mathbb{R}} = \{\bar{a} : a \in \mathbb{R}\}$ então a função barra $\begin{array}{c} - : \mathbb{R} \to \bar{\mathbb{R}} \\ a \leadsto \bar{a} \end{array}$ preserva soma e produto e de fato é um isomorfismo, ou seja $\mathbb{R} \simeq \bar{\mathbb{R}}$.

Agora, como em $L$, $\bar{x} = \alpha$ satisfaz a equação $z^2 + \bar{1} = 0$ pois $\bar{x}^2 + \bar{1} = \overline{x^2 + 1} = \bar{0}$ podemos então construir um isomorfismo $\psi$ de $\mathbb{C}$ sobre $L$ como segue:

$$\begin{aligned} \psi : \mathbb{C} &\to L, \text{ e portanto } \mathbb{C} \simeq L. \\ a + bi &\rightsquigarrow \bar{a} + \bar{b} \cdot \bar{x} \\ i &\rightsquigarrow \bar{x} \\ a &\rightsquigarrow \bar{a} \end{aligned}$$

EXEMPLO 2. Seja $A = \mathbb{Q}[x]$ e $I = A \cdot (x^2 - p)$ onde $p$ é um número primo positivo. É de fácil verificação que $K = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$ e $\sqrt{p}$ (aliás é o menor tal subcorpo). Vamos mostrar nesse exemplo que $A/I \simeq K$.

De fato, seja $L = A/I = \{\overline{p(x)} : p(x) \in A\}$, onde a barra é relativa a congruência módulo $I$. Como $\sqrt{p} \notin \mathbb{Q}$ sabemos que $x^2 - p$ é um polinômio irredutível em $\mathbb{Q}[x]$ e portanto $L$ é um corpo.

Se $p(x) \in A$ então pelo algorítmo da divisão existe $q(x)$, $r(x)$ em $\mathbb{Q}[x]$ tais que: $P(x) = q(x)(x^2 - p) + r(x)$, onde $r(x) = a + bx$, $a, b \in \mathbb{Q}$. Como no exemplo anterior segue imediatamente que $\overline{p(x)} = \overline{q(x)} \cdot \overline{(x^2 - p)} + \overline{r(x)} = \overline{r(x)} = \bar{a} + \bar{b} \cdot \bar{x}$ e portanto, $L = \{\bar{a} + \bar{b}\bar{x} : a, b \in \mathbb{Q}\}$.

De modo inteiramente análogo ao Exemplo 1 chegamos que a função barra: $\overline{\phantom{x}} : \mathbb{Q} \to \overline{\mathbb{Q}}$ é um isomorfismo ou seja $\mathbb{Q} \simeq \overline{\mathbb{Q}} = \{\bar{a} : a \in \mathbb{Q}\}$ e também $\bar{x} = \alpha$ satisfaz em $L$ a equação $z^2 - \bar{p} = 0$ pois $\bar{x}^2 - \bar{p} = \overline{x^2 - p} = \bar{0}$.

Assim podemos construir um isomorfismo $\psi : K \to L$ como segue:

$$\begin{aligned} \psi : K &\to L \\ a + b\sqrt{p} &\rightsquigarrow \bar{a} + \bar{b} \cdot \bar{x} \\ a &\rightsquigarrow \bar{a} \\ \bar{x} &\rightsquigarrow \sqrt{p} \end{aligned}$$

## EXERCÍCIOS

1. Seja $K$ um corpo e $f(x) \in K[x] - \{0\}$. Prove que, se $f(x)$ é um polinômio de grau $\geq 2$ e possui uma raiz $a \in K$ então $f(x)$ é redutível sobre $K$.
2. Mostre que todo polinômio $f(x) \in \mathbb{R}[x]$ de grau ímpar $\geq 3$ é redutível sobre $\mathbb{R}$.
3. Determine todos os $n$ de modo que $x^2 + \bar{2}$ divide $x^5 - \overline{10}x + \overline{12}$ em $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.
4. Determine todos os polinômios de grau 2 que sejam irredutível sobre $K = \mathbb{Z}_5$.
5. Determine todos os polinômios irredutíveis de grau $\leq 3$ sobre $K = \mathbb{Z}_3$.

6. Prove que se $J = \mathbb{R}[x] \cdot (x^2 + 1)$ é um ideal maximal de $\mathbb{R}[x]$ e identifique o corpo $\mathbb{R}[x]/J$.

7. Mostre que $x^3 + x + \bar{1} \in \mathbb{Z}_5[x]$ é irredutível sobre $\mathbb{Z}_5$.

8. Mostre que o polinômio $p(x) = x^3 - 2$ é irredutível sobre o corpo $\mathbb{Q}$.

9. Seja $K$ um corpo e $p(x) \in K[x]$ um polinômio irredutivel sobre $K$. Seja $f(x) \in K[x] - \{0\}$. Prove que, se $f(x) \backslash p(x)$ então ou $f(x) = a$ constante não nula ou $p(x) = b \cdot f(x)$ com $b \neq 0, b \in K$.

10. Prove que $f(x) = x^4 + 4$ é um polinômio redutível sobre o corpo $\mathbb{Q}$.

11. Seja $K$ um corpo e $f(x) \in K[x]$ um polinômio tal que $1 \leq \partial f(x) \leq 3$. Prove que ou $f(x)$ é irredutível sobre $K$ ou $f(x)$ possui uma raiz em $K$. E se grau de $f(x) = 4$?

12. Seja $f(x) \in \mathbb{R}[x]$ tal que $\partial f(x) = 2$.
Prove que, $f(x)$ é irredutível sobre $\mathbb{R} \Leftrightarrow f(x)$ pode ser escrito na forma $f(x) = (x - a)^2 + b^2$ onde $a, b \in \mathbb{R}$ e $b \neq 0$.

13. Seja $K$ um corpo e $p(x) \in K[x]$ um polinômio irredutível sobre $K$. Se $f(x), g(x) \in K[x]$ e $p(x) \backslash f(x) \cdot g(x)$, prove que $p(x) \backslash f(x)$ ou $p(x) \backslash g(x)$.
(Sugestão: veja a demonstração análoga feita para números primos no Parágrafo 5 do Capítulo 2).

## §5 Fatorização única

Se $u \in K - \{0\}$ e se $p_1(x), \ldots, p_m(x)$ são polinômios irredutíveis sobre $K$ vamos usar a expressão $f(x) = u \cdot p_1(x) \ldots p_m(x)$ de tal modo que incluiremos na mesma a possibilidade $f(x) = u$ no caso de $m = 0$.

**TEOREMA 5.** *Seja $K$ um corpo. Então todo polinômio $f(x) \in K[x] - \{0\}$ pode ser escrito na forma,*

$$f(x) = u \cdot p_1(x) \ldots p_m(x)$$

*onde $u \in K - \{0\}$ e $p_1(x), p_2(x), \ldots, p_m(x)$ são polinômios irredutíveis sobre $K$. (não necessariamente distintos).*

*Mais ainda, essa expressão é única a menos da constante $u$ e da ordem dos polinômios $p_1(x), \ldots, p_m(x)$.*

*Demonstração*. Seja $f(x) \in K[x] - \{0\}$.

Vamos provar por indução sobre $\partial f(x) = n$.

*Se* $n = 0$ $f(x) = u$ constante não nula. Assim, podemos assumir $\partial f(x) = n \geq 1$.

Vamos supor pela hipótese de indução que todo polinômio não nulo de grau menor que $n$ pode ser escrito na expressão desejada, e vamos demonstrar que $f(x)$ também pode ser escrito naquela expressão.

Suponhamos, por absurdo, que $f(x)$ não possa ser escrito como produto de irredutíveis. Então $f(x)$ é um polinômio redutível sobre $K$. Assim,

$$\exists\, g(x), h(x) \in K[x],\ 1 \leq \partial g(x) < n,\ 1 \leq \partial h(x) < n$$

tais que $f(x) = g(x) \cdot h(x)$.

Agora, por indução temos,

$$g(x) = a \cdot p_1(x) \dots p_r(x),\ a \in K - \{0\} \quad \text{e} \quad p_1(x), \dots, p_r(x)$$

polinômios irredutíveis sobre $K$. Analogamente,

$$h(x) = b \cdot p_{r+1}(x) \dots p_m(x),\ b \in K - \{0\} \quad \text{e} \quad p_{r+1}(x), \dots, p_m(x)$$

polinômios irredutíveis sobre $K$.

Assim, $f(x) = u \cdot p_1(x) \dots p_m(x)$, onde $u = ab \in K - \{0\}$ e $p_1(x), \dots, p_m(x)$ polinômios irredutíveis sobre $K$.

Vamos agora demonstrar a unicidade da expressão.

Suponhamos

$$f(x) = u \cdot p_1(x) \dots p_m(x) = u' \cdot p'_1(x) \dots p'_s(x)$$

onde $u, u' \in K - \{0\}$ e $p_1(x), \dots, p_m(x)$, $p'_1(x), \dots, p'_s(x)$ são polinômios irredutíveis sobre $K$.

Assim, temos,

$$p_1(x) \backslash p'_1(x) \dots p'_s(x)$$

e daí segue que $\exists\, u'_i \in K - \{0\}$ tal que $p'_i(x) = u'_i \cdot p_1(x)$ (nesse caso dizemos que $p'_i(x)$ e $p_1(x)$ são *associados* em $K[x]$).

Agora o teorema segue por indução sobre $m$.

Se $m = 1$ e $p_1(x)$ irredutível temos que necessáriamente $s = 1$ *e* $p_1(x)$ e $p'_i(x)$ são associados em $K[x]$.

Suponhamos $m > 1$. De $p'_i(x) = u'_i \cdot p_1(x)$ e sendo $K[x]$ um domínio temos que:

$$u \cdot p_2(x) \dots p_m(x) = u' \cdot u_i \cdot p'_1(x) \dots p_{i-1}(x) \cdot p_{i+1}(x) \dots p_s(x)$$

e daí segue pela hipótese de indução que $m - 1 = s - 1$ (isto é, $m = s$) e mais cada $p'_j(x)$ está associado com algum $p_i(x)$ através de uma constante, e isto termina a demonstração do teorema. ■

## EXERCÍCIOS

1. Se $K$ é um corpo. Prove que $K[x]$ satisfaz a *condição da cadeia ascendente de Ideais* (isto é, se $\{J_i\}_{i \in \mathbb{N}}$ é uma seqüência de ideais de $K[x]$ e $J_0 \subset J_1 \subset J_2 \subset \dots \subset J_n \subset \dots$ então $\exists\, m \in \mathbb{N}$ tal que
$$J_m = J_{m+1} = \dots = J_{m+s} = \dots \;\forall\, s \in \mathbb{N})$$
(Sugestão: Veja o Capítulo 2, Parágrafo 5).
2. Mostre com um contra-exemplo que se $K$ é um corpo então $K[x]$ não satisfaz a condição da cadeia descendente de ideais. (Sugestão: Seja $J_i = K[x] \cdot x^i$ o ideal gerado por $x^i$)
3. Use o teorema da fatorização única para definir M.D.C. e M.M.C. de polinômios.
4. Decomponha o polinômio $x^4 - 5x^2 + 6$ em produto de fatores irredutíveis sobre os seguintes corpos $K$:
(a) $K = \mathbb{Q}$.
(b) $K = \mathbb{Q}[\sqrt{2}]$
(c) $K = \mathbb{R}$.
5. Decomponha sobre o corpo $K = \mathbb{Z}_3$ os seguintes polinômios como produto de irredutíveis:
(a) $x^2 + x + \bar{1}$ ; (b) $x^3 + x + \bar{2}$;
(c) $\bar{2}x^3 + \bar{2}x^2 + x + \bar{1}$ ; (d) $x^4 + x^3 + x + \bar{1}$.
6. Prove que o polinômio $x^2 - \bar{3}$ é irredutível sobre o corpo $K = \mathbb{Z}_5$. Mais ainda, se $J = \mathbb{Z}_5[x] \cdot p(x)$, onde $p(x) = x^2 - \bar{3}$ então o corpo $\mathbb{Z}_5[x]/J$ possui exatamente 25 elementos.
7. Prove que o polinômio $p(x) = x^3 + x + \bar{1}$ é irredutível sobre $\mathbb{Z}_5$ e mostre que o corpo $\mathbb{Z}_5[x]/J$ possui exatamente 125 elementos onde $J = \mathbb{Z}_5[x] \cdot p(x)$ é o ideal principal de $\mathbb{Z}_5[x]$ gerado por $p(x) = x^3 + x + \bar{1}$.
8. Seja $p(x)$ um polinômio irredutível de grau $n$ sobre o corpo $\mathbb{Z}_p$, $p$ primo, e seja $J = \mathbb{Z}_p[x] \cdot p(x)$. Prove que $\mathbb{Z}_p[x]/J$ é um corpo contendo exatamente $p^n$ elementos.

9. (a) Defina a noção de irredutibilidade em um domínio $D$.
   (b) Prove que $\mathbb{Z}[\sqrt{5}] = D$ é um domínio onde não é válido o teorema da fatorização única.
   (Sugestão: Prove que $2, 3 + \sqrt{5}$ e $3 - \sqrt{5}$ são elementos irredutíveis em $D$ e verifique que $4 = 2 \cdot 2 = (3 + \sqrt{5}) \cdot (3 - \sqrt{5})$
   (c) Conclua então que em $D = \mathbb{Z}[\sqrt{5}]$ não existe Algorítmo da divisão de Euclides.

10. (a) Prove que $p(x) = x^2 + 1$ é irredutível sobre $K = \mathbb{Z}_7$ e construa um corpo contendo 49 elementos.
   (b) Prove que $p(x) = x^2 + 1$ é irredutível sobre $K = \mathbb{Z}_{11}$ e construa um corpo contendo 121 elementos.
   (c) Prove que $p(x) = x^2 + 1$ é redutível sobre $K = \mathbb{Z}_5$.
   (d) Prove que $p(x) = x^3 - 9$ é irredutível sobre o corpo $K = \mathbb{Z}_{31}$ e construa um corpo contendo $(31)^3$ elementos.
   (e) Prove que $p(x) = x^3 - 9$ é redutível sobre $\mathbb{Z}_{11}$.

## §6 O critério de Eisenstein

A verificação da irredutibilidade de um polinômio sobre um corpo é, em geral, um problema difícil. Veremos nesse parágrafo um teorema que nos dá condições suficientes para que um polinômio $f(x) \in \mathbb{Q}[x]$ seja irredutível sobre $\mathbb{Q}$. Claramente, multiplicando $f(x)$ pelo M.M.C. dos denominadores dos coeficientes de $f(x)$, podemos supor que $f(x) \in \mathbb{Z}[x]$. Vamos usar também a notação $a \nmid b$ significando que "$a$ não é um divisor de $b$".

Primeiramente vamos provar uma proposição (Lema de Gauss) que nos diz que irredutibilidade sobre $\mathbb{Z}$ de $f(x) \in \mathbb{Z}[x]$ é equivalente a irredutibilidade de $f(x)$ sobre $\mathbb{Q}$

**PROPOSIÇÃO 2** (Gauss). *Seja $f(x) \in \mathbb{Z}[x]$ tal que $f(x)$ é irredutível sobre $\mathbb{Z}$ então $f(x)$ é irredutível sobre $\mathbb{Q}$.*

*Demonstração.* Suponhamos que $f(x)$ seja irredutível sobre $\mathbb{Z}$ mas $f(x) = g(x) \cdot h(x)$, onde $g(x), h(x) \in \mathbb{Q}[x]$ e $1 \leq \partial g(x), \partial h(x) < \partial f(x)$.

Claramente existe inteiro positivo $m$ tal que $m \cdot f(x) = g_1(x) \cdot h_1(x)$ onde $g_1(x), h_1(x) \in \mathbb{Z}[x]$.

Assim temos,

$$g_1(x) = a_0 + a_1x + \ldots + a_rx^r, \; a_i \in \mathbb{Z}.$$
$$h_1(x) = b_0 + b_1x + \ldots + b_sx^s, \; b_i \in \mathbb{Z}.$$

Suponhamos agora que $p\backslash m$, $p$ primo. Vamos provar que $p\backslash a_i \; \forall \, i \in \{1, \ldots, r\}$ ou $p\backslash b \; \forall \, j \in \{1, \ldots, s\}$.

De fato, se $\exists \, i \in \{1, \ldots, r\}$ e $\exists \, j \in \{1, \ldots, s\}$ tais que $p\nmid a_i$ e $p\nmid b_j$ consideremos $i$ e $j$ menores possíveis com esta propriedade.

Ora, como $p\backslash m$ temos que $p$ divide o coeficiente de $x^{i+j}$ do polinômio $mf(x) = g_1(x) \cdot h_1(x)$, isto é, $p\backslash(b_0 \cdot a_{i+j} + b_1 \cdot a_{i+j-1} + \ldots + b_j \cdot a_i + \ldots + b_{i+j-1} \cdot a_1 + b_{i+j} \cdot a_0)$.

Pela nossa escolha de $i$ e $j$ temos que $p$ divide cada parcela, exceto $b_j \cdot a_i$, do coeficiente de $x^{i+j}$ de $g_1(x) \cdot h_1(x)$.

Como $p$ divide toda a expressão segue também que $p\backslash b_j \cdot a_i$ e como $p$ é um número primo temos que $p\backslash b_j$ ou $p\backslash a_i$ que é uma contradição.

Assim, se $p$ primo, $p\backslash m \Rightarrow p\backslash a_i \; \forall \, i \in \{1, \ldots, r\}$ ou $p\backslash b_j \; \forall \, j \in \{1, \ldots, s\}$.

Sem perda de generalidade, suponhamos que $p\backslash a_i \; \forall \, i \in \{1, 2, \ldots, r\}$.

Assim, $g_1(x) = p \cdot g_2(x)$ onde $g_2(x) \in \mathbb{Z}[x]$, e se $m = p \cdot m_1$ temos

$$p \cdot m_1 \, f(x) = p \cdot g_2(x) \cdot h_1(x)$$
$$m_1 f(x) = g_2(x) \cdot h_1(x).$$

Como o número de fatores primos de $m$ é finito prosseguindo no argumento acima (ou por indução sobre o número de fatores primos de $m$) chegaremos que:

$$f(x) = g^*(x) \cdot h^*(x) \quad \text{onde,}$$
$$g^*(x), h^*(x) \in \mathbb{Z}[x]$$

e $g^*(x)$ e $h^*(x)$ são multiplos racionais de $g(x)$ e $h(x)$, respectivamente, contradizendo a irredutibilidade de $f(x)$ sobre $\mathbb{Z}$. ■

**TEOREMA 6** (Critério de Eisenstein). *Seja* $f(x) = a_0 + a_1x + \ldots + a_nx^n$ *um polinômio em* $\mathbb{Z}[x]$.

*Suponhamos que exista um inteiro primo p tal que:*

(a) $p\nmid a_n$

(b) $p\backslash a_0, a_1, \ldots, a_{n-1}$

(c) $p^2\nmid a_0$.

*Então* $f(x)$ *é irredutível sobre* $\mathbb{Q}$.

*Demonstração.* Pela proposição anterior é suficiente provar que $f(x)$ é irredutível sobre $\mathbb{Z}$. Suponhamos por contradição que,

$$f(x) = g(x) \cdot h(x),\ g(x), h(x) \in \mathbb{Z}[x]$$

e

$$1 \leq \partial g(x), \partial h(x) < \partial f(x) = n$$

Seja,

$$g(x) = b_0 + b_1 x + \dots + b_r x^r \in \mathbb{Z}[x],\quad \partial g(x) = r$$
$$h(x) = c_0 + c_1 x + \dots + c_s x^s \in \mathbb{Z}[x],\quad \partial h(x) = s$$

Assim $n = r + s$.

Agora $b_0 \cdot c_0 = a_0$ e assim $p \backslash b_0$ ou $p \backslash c_0$ e como $p^2 \nmid a_0$ segue que $p$ divide apenas um dos inteiros $b_0, c_0$. Vamos admitir, sem perda de generalidade, que $p \backslash b_0$ e $p \nmid c_0$.

Agora $a_n = b_r \cdot c_s$ é o coeficiente de $x^n = x^{r+s}$ e portanto $p \nmid b_r$ e $p \backslash b_0$. Seja $b_i$ o primeiro coeficiente de $g(x)$ tal que $p \nmid b_i$.

Agora $a_i = b_0 \cdot c_i + b_1 \cdot c_{i-1} + \dots + b_i \cdot c_0$ e portanto como $p \backslash b_0, \dots, b_{i-1}, p \nmid b_i$ e $p \nmid c_0 \Rightarrow p \nmid a_i \Rightarrow i = n$ o que é um absurdo pois $1 \leq i \leq r < n$. ■

Vamos ver alguns exemplos de polinômios irredutíveis sobre $\mathbb{Q}$.

EXEMPLO 1. Seja $f(x) = x^3 + 2x + 10$. O critério de Einsenstein se aplica para o primo $p = 2$, portanto $f(x)$ é irredutível sobre $\mathbb{Q}$.

EXEMPLO 2. Agora, seja $p$ um número primo qualquer e seja $p(x) = x^n - p$ um polinômio de grau $n \geq 1$ sobre $\mathbb{Q}$. Claramente, o próprio primo $p$ se aplica no critério de Einsenstein, e portanto $p(x)$ é irredutível sobre $\mathbb{Q}$.

EXEMPLO 3. É de imediata verificação que se $K$ é um corpo e $a \in K$ então,

$$\psi : K[x] \to K[x]$$
$$f(x) \rightsquigarrow f(x + a)$$

é um automorfismo de $K[x]$.

Assim, não é difícil concluir que se $K$ é um corpo, $a \in K$ e $f(x) \in K[x]$ então $f(x)$ é irredutível sobre $K$ se e somente se $f(x + a)$ é irredutível sobre $K$. Vamos usar isto a seguir.

Seja $p$ um número primo $\geq 2$ e seja $q(x) \in \mathbb{Z}[x]$ o polinômio $q(x) = x^{p-1} + x^{p-2} + \ldots + x^p + x + 1$. Vamos provar que $q(x)$ é irredutível sobre $\mathbb{Q}$. Não podemos aplicar imediatamente o critério de Eisenstein, porém sabemos pelo argumento acima que $q(x)$ será irredutível sobre $\mathbb{Q}$ se $q(x + 1)$ for irredutível sobre $\mathbb{Q}$. Desenvolvendo $q(x + 1) = (x + 1)^{p-1} + (x + 1)^{p-2} + \ldots + (x + 1)^p + (x + 1) + 1$ é fácil de ver que o primo $p$ se aplica no critério de Eisenstein e portanto $q(x)$ é irredutível sobre $\mathbb{Q}$.

Agora vamos enunciar como proposição mais um critério de irredutibilidade sobre $\mathbb{Q}$.

PROPOSIÇÃO 3. *Seja $p$ um número primo e seja $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ o corpo contendo $p$ elementos.*

*Se $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$ vamos definir o polinômio $\bar{f}(x) \in \mathbb{Z}_p[x]$ do seguinte modo:*

$$\bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \ldots + \bar{a}_n x^n$$

*onde $\bar{a}_i = a_i + p \cdot \mathbb{Z}$ é a classe de equivalência, módulo $p$, cujo representante é $a_i \in \mathbb{Z}$.*

*Então,*

(a) $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ *define um homomorfismo (sobrejetivo) do domínio* $f(x) \rightsquigarrow \bar{f}(x)$

$\mathbb{Z}[x]$ *sobre o domínio* $\mathbb{Z}_p[x]$.

(b) *Se $p \nmid a_n$ e $\bar{f}(x)$ é irredutível sobre $\mathbb{Z}_p$ então $f(x)$ é irredutível sobre $\mathbb{Q}$. (Observe que se $f(x)$ é mônico, então $p \nmid a_n = 1$ é sempre satisfeita).*

*Demonstração.* (a) a demonstração desse item é direta e deixamos como exercício.

(b) suponhamos $f(x) = a_0 + a_1 x + \ldots + a_n x^n$; grau $f = n$ e $p$ primo $p \nmid a_n$.

Suponhamos que $f(x) \in \mathbb{Z}[x]$ é redutível sobre $\mathbb{Q}$. Então sabemos (Lema de Gauss) que

$$\exists\, g(x) = b_0 + b_1 x + \ldots + b_r x^r \in \mathbb{Z}[x] \text{ grau } g(x) = r,\ 1 \leq r < n$$

e

$$\exists\, h(x) = c_0 + c_1 x + \ldots + c_s x^s \in \mathbb{Z}[x] \text{ grau } h(x) = s,\ 1 \leq s < n$$

tais que $f(x) = g(x) \cdot h(x)$.

Imediatamente segue que:

$$\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x)$$

onde $\bar{g}(x) \in \mathbb{Z}_p[x]$ e $\bar{h}(x) \in \mathbb{Z}_p[x]$.

Mais ainda, como $a_n = b_r \cdot c_s$ e $p \nmid a_n$ segue que $p \nmid b_r$ e $p \nmid c_s$ e portanto $\bar{b}_r \neq \bar{0}$ e $\bar{c}_0 \neq \bar{0}$, isto é, grau $\bar{g}(x) = r$ e grau $\bar{h}(x) = s$ e portanto $\bar{f}(x)$ é redutível sobre $\mathbb{Z}_p$ e isto demonstra a proposição. ■

EXEMPLO 4. Seja $f(x) = x^4 + 10x^3 + 15x^2 + 5x + 12 \in \mathbb{Z}[x]$.

Vamos provar que $f(x)$ é irredutível sobre $\mathbb{Q}$.

Considere $p = 5$ e $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ então $\bar{f}(x) = x^4 + \bar{2} \in \mathbb{Z}_5[x]$. Como $5 \nmid 1$ pela proposição anterior é suficiente provarmos que $\bar{f}(x) = x^4 + \bar{2}$ é irredutível sobre $\mathbb{Z}_5$.

A primeira observação que fazemos é que $x^4 + \bar{2} = \bar{f}(x)$ não possui raízes em $\mathbb{Z}_5$. Assim a única possibilidade de fatorarmos $\bar{f}(x) = x^4 + \bar{2}$ seria a seguinte:

$$x^4 + \bar{2} = (ax^2 + bx + c) \cdot (a'x^2 + b'x + c')$$

onde $a, b, c, a', b', c' \in \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. Porém desenvolvendo as contas é fácil concluir pela impossibilidade dessa última fatoração.

Assim,

$$f(x) = x^4 + 10x^3 + 15x^2 + 5x + 12$$

é irredutível sobre $\mathbb{Q}$.

## EXERCÍCIOS

1. Prove que os seguintes polinômios $f(x) \in \mathbb{Z}[x]$ são irredutíveis sobre $\mathbb{Q}$.
   (a) $f(x) = x^4 + 2x^3 + 2x^2 + 2x + 2$
   (b) $f(x) = x^7 - 31$
   (c) $f(x) = x^6 + 15$
   (d) $f(x) = x^3 + 6x^2 + 5x + 25$
   (e) $f(x) = x^4 + 8x^3 + x^2 + 2x + 5$
   (f) $f(x) = x^4 + 10x^3 + 20x^2 + 30x + 22$

2. Determine quais dos seguintes polinômios são irredutíveis sobre $\mathbb{Q}$:
   (a) $x^3 - x + 1$ ; (b) $x^3 + 2x + 10$;
   (c) $x^3 - 2x^2 + x + 15$ ; (d) $x^4 + 2$
   (e) $x^4 - 2$ ; (f) $x^4 - x + 1$.

3. Seja $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ um polinômio de grau $n$. Prove que, se $f(x)$ é mônico, então toda raiz racional de $f(x)$ é inteira.

4. Prove que $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$ é irredutível sobre $\mathbb{R} \Leftrightarrow b^2 - 4ac < 0$.

5. Determine quais dos seguintes polinômios sobre os seguintes corpos $K$ são irredutíveis:
   (a) $x^7 + 22x^3 + 11x^2 - 44x + 33$, $K = \mathbb{Q}$
   (b) $x^3 - 7x^2 + 3x + 3$, $K = \mathbb{Q}$
   (c) $x^4 = \bar{5}$, $K = \mathbb{Z}_{17}$
   (d) $x^3 - \bar{5}$, $K = \mathbb{Z}_{11}$
   (e) $x^4 + \bar{7}$, $K = \mathbb{Z}_{17}$

CAPÍTULO V

# EXTENSÕES ALGÉBRICAS DOS RACIONAIS

O objetivo principal desse capítulo será a construção de corpos $K, \mathbb{Q} \subset K \subset \mathbb{C}$ através do processo de adjunção de raízes de um polinômio. Vamos também provar alguns resultados que serão úteis no desenvolvimento da Teoria de Galóis.

## §1 Adjunção de raízes

Neste parágrafo, $K$ representa um corpo e $L \supset K$ uma extensão de $K$.

Dizemos que $\alpha \in L$ é *algébrico sobre* $K$ se $\exists\, f(x) \in K[x] - \{0\}$ tal que $f(\alpha) = 0$. Caso contrário dizemos que $\alpha$ é *transcendente sobre* $K$.

Os elementos algébricos (transcendentes) sobre $Q$ são ditos simplesmente algébricos (transcendentes). Assim, $\sqrt[3]{2}$ é um elemento algébrico enquanto $\pi$ é um elemento transcendente. Se $\alpha \in K$, evidentemente $\alpha$ é algébrico sobre $K$ pois é raiz de $p(x) = x - \alpha \in [x]$.

Se $\forall\, \alpha \in L \supset K$, $\alpha$ é algébrico sobre $K$ então $L \supset K$ diz-se uma *extensão algébrica.*

Seja $\alpha \in L$ algébrico sobre $K$ e seja $p(x)$ um polinômio em $K[x]$, mônico, de menor grau tal que $p(\alpha) = 0$. Pela minimalidade do grau de $p(x)$ segue claramente que $p(x)$ é o único polinômio mônico irredutível em $K[x]$ tal que $p(\alpha) = 0$, o qual denotaremos por $p(x) = irr(\alpha, K)$.

Se $\alpha \in L \supset K$ definimos $K[\alpha] = \{f(\alpha) : f(x) \in K[x]\}$, e é de fácil verificação que $K[\alpha]$ é um subdomínio de $L$ que contém $K$.

Antes de enunciarmos o próximo teorema vamos dar alguns exemplos.

EXEMPLO 1. Se $\alpha = \sqrt{2} \in L = \mathbb{R} \supset \mathbb{Q} = K$ vamos mostrar que $K[\alpha] = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. De fato, por definição temos $\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}) : f(x) \in \mathbb{Q}[x]\}$. Agora se $f(x) \in \mathbb{Q}[x]$, segue pelo algorítmo da divisão que existe $q(x), r(x) \in \mathbb{Q}[x]$ tais que $f(x) = q(x)(x^2 - 2) + r(x)$, onde $r(x) = a + bx, a, b \in \mathbb{Q}$, e daí vem que $f(\sqrt{2}) = r(\sqrt{2}) = a + b\sqrt{2},\ a, b \in \mathbb{Q}$.

EXEMPLO 2. Se $\alpha = \sqrt[3]{2} \in L = \mathbb{R} \supset \mathbb{Q} = K$ vamos mostrar que $K[\alpha] = \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}$.
De fato,

$$\mathbb{Q}[\sqrt[3]{2}] = \{f(\sqrt[3]{2}) : f(x) \in \mathbb{Q}[x]\}.$$

Agora, se $f(x) \in \mathbb{Q}[x]$ existe $q(x), r(x) \in \mathbb{Q}[x]$ tais que $f(x) = q(x)(x^3 - 2) + r(x)$, onde $r(x) = a + bx + cx^2, a, b, c \in \mathbb{Q}$.

Daí vem imediatamente:

$$\mathbb{Q}[\sqrt{2}] = \{a + b(\sqrt[3]{2}) + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}.$$

Provaremos mais adiante que se $\alpha \in L \supset K$ é um elemento algébrico sobre $K$ então $K[\alpha]$ é um subcorpo de $L$. Em particular, $\mathbb{Q}[\sqrt[3]{2}]$ e $\mathbb{Q}[\sqrt[3]{2}]$ são exemplos de corpos.

O próximo teorema é conseqüência imediata do 1.º teorema de homorfismo de anéis e deixamos a demonstração para o leitor.

TEOREMA 1. *Se $\alpha \in L \supset K$ e se Se $\Psi : K[x] \to L$ é definida por $\Psi(f(x)) = f(\alpha)$, então $\Psi$ é um homorfismo tal que:*

(i) *$Im\ \Psi = K[\alpha]$, $K \subset K[\alpha] \subset L$.*

(ii) *$\alpha$ é transcendente sobre $K \Leftrightarrow N(\Psi) = \{0\}$.*

(iii) *se $\alpha$ é algébrico sobre $K$ e $p(x) = \mathrm{irr}(\alpha, K)$ então $N(\Psi) = K[x] \cdot p(x)$ é um ideal maximal de $K[x]$.*

(iv) *$K[x]/N(\Psi) \simeq K[\alpha]$.*

*Demonstração.* Essa demonstração é conseqüência direta do 1.º teorema de homorfismo de anéis e das definições dadas nesse parágrafo. ■

COROLÁRIO 1. *Seja $\alpha \in L \supset K$. (a) Se $\alpha$ é algébrico sobre $K$ então $K[\alpha]$ é um subcorpo de $L$ que contém $K$.*

(b) *Se $\alpha$ é transcendente sobre $K$ então $K[\alpha]$ é um subdomínio de $L$ isomorfo ao domínio $K[x]$ dos polinômios em uma indeterminada $x$.*

*Demonstração.* (a) Segue imediatamente de (iii) e (iv) do Teorema 1.
(b) Segue imediatamente de (ii) e (iv) do Teorema 1. ■

COROLÁRIO 2. *Se $\alpha, \beta \in L \supset K$ são raízes de um mesmo polinômio irredutível sobre $K$, então $K[\alpha]$ e $K[\beta]$ são corpos isomorfos.*

*Demonstração.* De nossas hipóteses segue imediatamente que $p(x) = irr(\alpha, K) = irr(\beta, K)$. Agora, pelos ítens (iii) e (iv) do Teorema anterior temos, $J = K[x] \cdot p(x)$ e $K[\alpha] \simeq K[x]/J \simeq K[\beta]$ são corpos. ■

PROPOSIÇÃO 1. *Seja $L \supset K$, $\alpha \in L$ algébrico sobre $K$. Se o grau do polinômio $irr(\alpha, K)$ é $n$, então* (a) $\forall f(x) \in K[x]$, $f(\alpha)$ *pode ser expresso de modo único na forma* $f(\alpha) = a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1}$, *onde* $a_i \in K$.

(b) $K[\alpha] = \{a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1} : a_i \in K\}$ *é um subcorpo de $L$ que contém $K$.*

(c) *se $K = \mathbb{Z}_p$ então $K[\alpha]$ é um corpo contendo exatamente $p^n$ elementos.*

*Demonstração.* Seja $p(x) = irr(\alpha, K)$. Por hipótese, grau de $p(x)$ é igual a $n$.

(a) se $f(x) \in K[x]$ então pelo algoritmo da divisão $\exists\, q(x), r(x) \in K[x]$ tais que: $f(\alpha) = q(\alpha) \cdot p(\alpha) + r(\alpha)$ onde $r(x) = 0$ ou $\partial(r(x)) < \partial p(x)$. Assim $r(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$ onde $a_i \in K$, $i = 0, 1, \ldots, n-1$. Agora temos,

$$f(\alpha) = q(\alpha) \cdot p(\alpha) + r(\alpha) \text{ e } p(\alpha) = 0 \Rightarrow f(\alpha) = r(\alpha)$$

ou seja $f(\alpha) = a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1}$.

Para demonstrar a unicidade da expressão temos: se $f(\alpha) = a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1} = b_0 + b_1 \alpha + \ldots + b_{n-1} \alpha^{n-1}$ $a_i, b_i \in K$ $\forall\, i \in \{1, \ldots, n-1\}$ segue imediatamente que o polinômio $q(x) \in K[x]$ onde $q(x) = (a_0 - b_0) + (a_1 - b_1)x + \ldots + (a_{n-1} - b_{n-1})x^{n-1}$ é tal que $q(\alpha) = 0$ e $\partial q(x) < n = \partial(irr(\alpha, K))$. Assim $q(x) = 0$ e daí segue $a_i = b_i$ $\forall\, i \in \{1, \ldots, n-1\}$.

(b) esse item é conseqüência imediata do item anterior.

(c) para demonstrar esse item basta observar que pelos itens anteriores temos:

$$\mathbb{Z}_p[\alpha] = \{a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1} : a_i \in \mathbb{Z}_p\}.$$

Assim existe uma correspondência bijetiva entre $\mathbb{Z}_p[\alpha]$ e o conjunto de todas as n-uplas $(a_0, a_1, \ldots, a_{n-1})$ onde cada $a_i \in \mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ e isto demonstra o item (c). ■

EXEMPLOS. Seja $\alpha = \sqrt[n]{p} \in \mathbb{R}$, $n$ inteiro $\geq 2$ e $p$ primo $\geq 2$. Então $\alpha$ é uma raiz real do polinômio $x^n - p$ que é, pelo critério de Eisenstein, irredutível sobre $\mathbb{Q}$.

Assim $x^n - p = \text{irr}(\alpha, \mathbb{Q})$ e temos, $\mathbb{Q}[\alpha]$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$ e mais ainda, $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}, i = 0, \ldots, n-1\}$.

Por exemplo,

$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] = \{a_0 + a_1\sqrt{2} : a_0, a_1 \in \mathbb{Q}\} \subset \mathbb{R}$

$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 : a_0, a_1, a_2 \in \mathbb{Q}\} \subset \mathbb{R}$

$\mathbb{Q} \subset \mathbb{Q}[\sqrt[4]{3}] = \{a_0 + a_1\sqrt[4]{3} + a_2(\sqrt[4]{3})^2 + a_3(\sqrt[4]{3})^3 : a_0, a_1, a_2, a_3 \in \mathbb{Q}\} \subset \mathbb{R}$

Agora se $\beta$ é uma raiz cúbica complexa de 2, $\beta \notin \mathbb{R}$, temos que,

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R},\ \mathbb{Q} \subset \mathbb{Q}[\beta] \subset \mathbb{C}$$

e mais ainda $\mathbb{Q}[\sqrt[3]{2}] \simeq \mathbb{Q}[\beta]$ pois $\sqrt[3]{2} \in \mathbb{R}$ e $\beta \in \mathbb{C}$ são raizes do mesmo polinômio indutível $x^3 - 2$ sobre $\mathbb{Q}$.

Se $p_i$ é um número primo $\geq 2$ vamos definir $\alpha_i$ por $\alpha_i = \sqrt[2^i]{p} \in \mathbb{R}$. Observe que $\alpha_i \in \mathbb{R}$ é raiz do polinômio $x^{2^i} - p$ que é irredutível (Eisenstein) sobre $\mathbb{Q}, \forall i \in \mathbb{N}$.

Assim temos, os corpos $K_i = \mathbb{Q}[\alpha_i]$ onde $\mathbb{Q} \subset K_i \subset \mathbb{R}$, e ainda mais, $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_i \subset \ldots \subset \mathbb{R}$ é uma cadeia ascendente de subcorpos de $\mathbb{R}$ e portanto $\bigcup_{i=0}^{\infty} K_i$ é também um subcorpo de $\mathbb{R}$.

Agora, seja $K = \mathbb{Z}_p$ então $\mathbb{Z}_p(x)$, o corpo de frações de $\mathbb{Z}_p[x]$, é um corpo infinito de característica $p$ e mais $x \in \mathbb{Z}_p(x)$ é um elemento transcendente sobre $\mathbb{Z}_p$. Vamos provar em seguida que todo corpo finito $F$ de característica $p$ cujo corpo primo é $P \simeq \mathbb{Z}_p$ é algébrico sobre $P$. De fato, se $\alpha \in F$ temos que $P[\alpha]$ é um subdomínio de $F$ e como $F$ é finito temos que $P[\alpha]$ é um domínio finito e portanto um corpo. Pelo Corolário 1 desse parágrafo segue imediatamente que $\alpha$ é algébrico sobre $P$.

Finalmente, observe que $\mathbb{R}[i] = \mathbb{C}$ e $\mathbb{Q}[\pi] \simeq \mathbb{Q}[x]$.

## §2 Corpo de decomposição de um polinômio

Neste parágrafo consideraremos $K$ um subcorpo de $\mathbb{C}$. Vamos também admitir que $\mathbb{C}$ é um corpo algébricamente fechado, fato esse conhecido como o "teorema fundamental da Álgebra" e primeiro demostrado por Gauss, em 1799, em sua tese de doutoramento na Universidade de Helmstadt. Como referências podemos citar: W. K. Clifford, Mathematical Papers 1968 ou L. H. Jacy Monteiro, Elementos de Álgebras – IMPA 1969. Assim, se $f(x) \in K[x]$ é um polinômio de

grau $n \geq 1$ e $\alpha_1, \alpha_2, \ldots, \alpha_r$ são todas as distintas raízes de $f(x)$ em $\mathbb{C}$ temos que,

$$f(x) = c \cdot (x - \alpha_1)^{m_1} \ldots (x - \alpha_r)^{m_r} \text{ em } \mathbb{C}[x]$$

onde $c \in K$ e $r, m_1, \ldots, m_r$ são inteiros positivos.

O inteiro $m_i$ chama-se *multiplicidade da raiz* $\alpha_i$. Se $m_i = 1$ dizemos que $\alpha_i$ é uma *raiz simples* de $f(x)$.

Se $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$ definimos $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1} \in K[x]$ o qual chamamos *a derivada de* $f(x)$. Observe que se $\partial f(x) = n \geq 1$ então $f'(x) \neq 0$ e $\partial f'(x) = n - 1$.

Se $f(x), g(x) \in K[x]$ e $a \in K$ segue imediatamente as seguintes regras:

$$(f(x) + g(x))' = f(x)' + g(x)'$$
$$(a \cdot f(x))' = a \cdot f(x)'$$
$$(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x).$$

PROPOSIÇÃO 2. *Seja* $f(x) \in K[x]$, $\partial f(x) = n \geq 1$ e $\alpha \in \mathbb{C}$ *uma raiz de* $f(x)$. *Então,*

(a) $\alpha$ *é raiz simples de* $f(x) \Leftrightarrow f(\alpha) = 0$ *e* $f'(\alpha) \neq 0$.

(b) *se* $f(x)$ *é irredutível sobre* $K$ *então todas as raízes de* $f(x)$ *são simples.*

*Demonstração.* (a) Para a demonstração deste item basta observar que se $\alpha \in \mathbb{C}$ é uma raiz de $f(x)$ de multiplicidade $m \geq 1$ então, em $\mathbb{C}[x]$, temos a seguinte fatorização:

$$f(x) = (x - \alpha)^m \cdot g(x) \text{ onde } g(x) \in \mathbb{C} \text{ e } g(\alpha) \neq 0.$$

Agora em $\mathbb{C}[x]$, usando a regra da derivada de um produto temos,

$$0 \neq f'(x) = m \cdot (x - \alpha)^{m-1} \cdot g(x) + (x - \alpha)^m \cdot g'(x).$$

Portanto, como $g(\alpha) \neq 0$, temos claramente que $m \cdot (x - \alpha)^{m-1}$ não é o polinômio nulo e mais, $f'(\alpha) = 0 \Leftrightarrow m \geq 2$. E isto demonstra o item a).

(b) seja $f(x) \in K[x]$ um polinômio irredutível sobre $K$ e $\alpha \in \mathbb{C}$ uma raiz de $f(x)$ de multiplicidade $m$. Vamos provar que $m = 1$.

Seja $p(x) = \mathrm{irr}(\alpha, K)$. Pelo algoritmo de Euclides segue que $\exists\, q(x), r(x) \in K[x]$ tais que,

$$f(x) = q(x) \cdot p(x) + r(x), \text{ onde } r(x) = 0 \text{ ou } \partial r(x) < \partial p(x).$$

Como $r(\alpha) = f(\alpha) - q(\alpha) \cdot p(\alpha) = 0$ segue pela minimalidade do grau de $p(x) = \mathrm{irr}(\alpha, K)$ que $r(x) = 0$ e $f(x) = q(x) \cdot p(x)$. Portanto, pela ir-

redutibilidade de $f(x)$, segue que $\exists\, a \in K$ tal que $q(x) = a \in K$ e $f(x) = a \cdot p(x)$.

Agora se $m > 1$ segue do item (a) que $f'(\alpha) = a \cdot p'(\alpha) = 0$, ou seja $p'(\alpha) = 0$ o que contradiz a minimalidade do grau de $p(x)$. Assim, $m = 1$ e a proposição está provada. ■

Chamamos *corpo de decomposição de um polinômio* $f(x) \in K[x]$ sobre $K$, que denotaremos por $L = \text{Gal}(f, K)$ ao menor subcorpo de $\mathbb{C}$ que contém $K$ e todas as raizes de $f(x)$ em $\mathbb{C}$. Observe que tal menor subcorpo existe e é igual a interseção de todos os subcorpos de $\mathbb{C}$ contendo $K$ e todas as raízes de $f(x)$ em $\mathbb{C}$.

Sejam $f(x) \in K[x]$ e $\alpha_1, \ldots, \alpha_r$ as distintas raizes de $f(x)$ em $\mathbb{C}$. Veremos agora um modo construtivo de definir $\text{Gal}(f, K)$.

Consideremos,

$$K_0 = K \subset K_1 = K[\alpha_1] \subset K_2 = K_1[\alpha_2] \subset \ldots \subset K_r = K_{r-1}[\alpha_r].$$

Claramente $K_i$ é o menor subcorpo de $\mathbb{C}$ contendo $K$ e $\alpha_1, \ldots, \alpha_i$ e portanto $K_r = K_{r-1}[\alpha_r] = \text{Gal}(f, K)$.

Denotando $K_r = K[\alpha_1, \ldots, \alpha_r]$ temos $\text{Gal}(f, K) = K[\alpha_1, \ldots, \alpha_r]$. É imediato que qualquer que seja a ordem em que pegamos as raízes $\alpha_1, \ldots, \alpha_r$ ainda assim esse processo, chamado *adjunção de raizes*, nos levaria a $\text{Gal}(f, K)$.

EXEMPLOS. As vezes para pegarmos todas as raízes $\alpha_1, \ldots, \alpha_r$ não precisamos das $r$ etapas. De fato, as vezes uma etapa é suficiente. Ou seja, ao ajuntarmos uma raiz $\alpha_i$ as demais ficam automaticamente incluídas.

Por exemplo, sejam $1 = \alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ as $n$ raízes em $\mathbb{C}$ do polinômio $x^n - 1 \in \mathbb{Q}[x]$ onde $n \geq 1$. É fácil provar que, se $\alpha = \cos \frac{2\pi}{n} + i \operatorname{sen} \frac{2\pi}{n} \in \mathbb{C}$ então $\alpha^n = 1$ e mais ainda: $1 = \alpha^0, \alpha_1 = \alpha^1, \alpha^2, \ldots, \alpha^{n-1}$ são as $n$ distintas raízes de $x^n - 1$ em $\mathbb{C}$. Assim, $\alpha_i = \alpha^i \in \mathbb{Q}[\alpha]\ \forall\, i \in \{0, \ldots, n-1\}$ e portanto,

$$\text{Gal}(x^n - 1, \mathbb{Q}) = \mathbb{Q}[\alpha_1].$$

Agora seja $\alpha = \sqrt[3]{2} \in \mathbb{R}$ e $\beta = \sqrt[3]{2} \cdot \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right) \in \mathbb{C}$ uma raiz complexa de $x^3 - 2 \in \mathbb{Q}[x]$. É fácil verificarmos que $\alpha, \beta, \bar{\beta} = \sqrt[3]{2}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2} i\right)$ são as 3 distintas raízes de $x^3 - 2$ em $\mathbb{C}$ e nesse caso necessitamos de duas etapas, isto é,

$$\mathrm{Gal}(x^3 - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, \beta].$$

Vamos mostrar agora que se $\alpha = \sqrt[n]{2} \in \mathbb{R}$ e $u = \cos \dfrac{2\pi}{n} + i \operatorname{sen} \dfrac{2\pi}{n}$ (raiz n-ésima da unidade) então $\mathrm{Gal}(x^n - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, u] = \mathbb{Q}[\alpha, \beta]$ onde $\beta = \alpha \cdot u$ é uma raiz de $x^n - 2$ em $\mathbb{C}$. Primeiramente é claro que se $u^n = 1$ e $\alpha^n = 2$ então $\beta^n = 2$ onde $\beta = \alpha \cdot u$ e mais $\mathbb{Q}[\alpha, u] = \mathbb{Q}[\alpha, \beta]$. Pode-se também provar que:

$$\alpha, \alpha u, \alpha u^2, \ldots, \alpha u^{n-1}$$

são das distintas $n$ raízes de $x^n - 2$ em $\mathbb{C}$. Observe que $1, u, u^2, \ldots, u^{n-1}$ são as distintas $n$ raízes de $x^n - 1$ em $\mathbb{C}$.

Agora deixamos como exercício provar que $\mathrm{Gal}(x^n - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, u] = \mathbb{Q}[\alpha, \beta]$.

## EXERCÍCIOS

1. Construir o corpo de decomposição sobre $\mathbb{Q}$, dos seguintes polinômios:

$$x^4 - 3,\ x^5 - 3,\ x^6 - 2 \text{ e } x^7 - 5.$$

2. Defina a noção de derivada de um polinômio sobre um corpo arbitrário e mostre que sobre $\mathbb{Z}_p$ temos a possibilidade de $f'(x) = 0$ onde $f(x)$ é um polinômio não constante sobre $\mathbb{Z}_p$.

3. Seja $K$ um corpo de característica zero e $f(x) \in K[x]$. Prove que se $f'(x) = 0$ então $f(x)$ é um polinômio constante.

4. Sejam $p$ e $q$ números primos $\geq 2$ e $\alpha, \beta$ definidos por: $\alpha = \sqrt[p]{q} \in \mathbb{R}$ e $u = \left(\cos \dfrac{2\pi}{p} + i \cdot \operatorname{sen} \dfrac{2\pi}{p}\right) \in \mathbb{C}$.

   Prove que:

   (a) $\alpha, \alpha u, \alpha u^2, \ldots, \alpha u^{p-1}$ são as $p$ distintas raízes de $x^p - q$ em $\mathbb{C}$.

   (b) $\mathrm{irr}(\alpha, \mathbb{Q}) = x^p - q$ e $irr(u, \mathbb{Q}) = x^{p-1} + x^p + \ldots + x + 1$

   (c) $\mathrm{Gal}(x^p - q, \mathbb{Q}) = \left\{ \Sigma \lambda_{ij} \alpha^i u^j : \lambda_{ij} \in \mathbb{Q}, \begin{array}{c} 0 \leq i \leq p-1 \\ 0 \leq j \leq p-2 \end{array} \right\}$

   (Sugestão: $\mathrm{Gal}(x^p - q, \mathbb{Q}) = \mathbb{Q}[\alpha, u]$)

5. Se $a \in K, f(x), g(x) \in K[x]$, onde $K$ é um corpo, então são válidas as seguintes regras de derivação:

   (a) $(f(x) + g(x))' = g'(x) + g'(x)$;

   (b) $(a \cdot f(x))' = a \cdot f'(x)$;

   (c) $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$.

6. Sejam $\alpha = \sqrt[3]{2} \in \mathbb{R}$ e $\beta = \sqrt[3]{2} \cdot \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right) \in \mathbb{C}$.
Então, prove que:
(a) $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[\beta]$
(b) $|\mathrm{Aut}\ \mathbb{Q}[\alpha]| = 1$ (onde $|X|$ = número de elementos do conjunto $X$).
(c) $\mathrm{Gal}(x^3 - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\alpha, \bar{\beta}] = \mathbb{Q}[\beta, \bar{\beta}]$.
(d) se $L = \mathrm{Gal}(x^3 - 2m\ \mathbb{Q})$ então $|\mathrm{Aut}\ L| = 6$.
(observe que se $\sigma \in \mathrm{Aut}\ L$ e $u^3 = 2$ então $\sigma(u)^3 = 2$)

7. Se $L \supset K$ é uma extensão de $K$ onde $K$ é um subcorpo de $\mathbb{C}$, então vamos definir o seguinte conjunto:
$$\mathrm{Aut}_K L = \{\sigma = \mathrm{Aut}\ L : \sigma(a) = a\ \forall\ a \in K\}.$$
Seja $f(x) \in K[x]$ e $\alpha \in L$ uma raiz de $f(x)$ em $L$, prove que: $\sigma(\alpha)$ é também uma raiz de $f(x)$ em $L$, $\forall\ \sigma \in \mathrm{Aut}_K L$.

8. Prove que:
(a) $|\mathrm{Aut}\ \mathbb{Q}[\sqrt[4]{2}]| = 2$
(b) $\mathrm{Gal}(x^4 - 2, \mathbb{Q}) = \mathbb{Q}[\sqrt[4]{2}, i]$
(c) se $L = \mathrm{Gal}(x^4 - 2, \mathbb{Q})$ então $|\mathrm{Aut}\ L| = 8$.

9. Seja $L$ um corpo qualquer e $P$ o corpo primo de $L$. Prove que $\forall\ \sigma \in \mathrm{Aut}\,(L)$ então $\sigma(a) = a\ \forall\ a \in P$. Em particular, se $L \supset \mathbb{Q}$ então $\mathrm{Aut}\ L = \mathrm{Aut}_{\mathbb{Q}} L$.

10. Seja $f(x) \in \mathbb{Q}[x]$ e $L = \mathrm{Gal}(f, \mathbb{Q})$. Então $\alpha$ raiz de $f(x)$ e $\sigma \in \mathrm{Aut}\ L \Rightarrow \sigma(\alpha)$ é raiz de $f$. Mais ainda, se $f$ é irredutível sobre $\mathbb{Q}$ temos $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[\sigma(\alpha)]$.

11. Prove que:
(a) $\mathrm{Gal}(x^5 - 1, \mathbb{Q}) = \mathbb{Q}[\alpha]$ onde $\alpha \neq 1$ e $\alpha^5 = 1$.
(b) $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 : a_i \in \mathbb{Q}, i = 0, 1, 2, 3\}$ onde $\alpha^5 = 1$ e $\alpha \neq 1$.
(c) se $L = \mathrm{Gal}(x^5 - 1, \mathbb{Q})$ então $|\mathrm{Aut}\ L| = 4$.

12. Seja $p$ um número primo $\geq 2$. Prove que:
(a) $\mathrm{Gal}(x^p - 1, \mathbb{Q}) = \mathbb{Q}[\alpha]$ onde $\alpha^p = 1$ e $\alpha \neq 1$
(b) $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \ldots + a_{p-2}\alpha^{p-2} : a_i \in \mathbb{Q}, i = 0, \ldots, p = 2\}$.
(c) se $L = \mathrm{Gal}(x^p - 1, \mathbb{Q})$ então $|\mathrm{Aut}\ L| = p - 1$.

13. Mostre que no plano $\mathbb{R}^2$ as raízes n-ésimas da unidade são vértices de um polígono regular de $n$ lados inscritos em uma circunferência de raio 1.
Generalize o resultado para as raízes n-ésimas de 2. Faça os desenhos para $n = 3, 4, 5$ e 6.

## §3 Grau de uma extensão

Neste parágrafo vamos necessitar de algumas noções básicas de Álgebra Linear, como espaço vetorial e base. Seremos o mais sucinto possível e deixaremos como exercício demonstrações de algumas proposições elementares, as quais poderão ser encontradas em qualquer livro introdutório de Álgebra Linear.

Seja $K$ um corpo qualquer e seja $V$ um conjunto não vazio onde está definida uma operação soma. Suponhamos também que esteja definida, uma operação de elementos de $K$ por elementos de $V$. Assim, estão definidas:

$$+ : V \times V \to V \qquad \text{e } K \times V \to V$$
$$(u, v) \rightsquigarrow u + v \qquad (\lambda, v) \rightsquigarrow \lambda v$$

Dizemos que $V$ munido dessas operações *é um espaço vetorial sobre o corpo* $K$ se as seguintes propriedades são verificadas quaisquer que sejam $u, v, w \in V$ e $\lambda, \mu \in K$:

$E_1$) $u + (v + w) = (u + v) + w$ (associatividade da soma)

$E_2$) $\exists\, 0 \in V$ tal que $u + 0 = 0 + u = u$ (existência de elemento neutro para a soma)

$E_3$) $\forall x \in V\ \exists\, y \in V$ tal que $x + y = y + x = 0$ (existência de inverso aditivo)

$E_4$) $u + v = v + u$ (comutatividade da soma)

$E_5$) $1v = v$ onde 1 é a unidade do corpo $K$.

$E_6$) $\lambda(u + v) = \lambda u + \lambda v$ e $(\mu + \lambda)u = \mu u + \lambda u$

$E_7$) $\lambda(\mu v) = \mu(\lambda v) = (\lambda u)v$.

EXEMPLO 1. Seja $K$ um corpo qualquer e $K^n = K \times \ldots \times K$ o conjunto de todas as n-uplas $(a_1, \ldots, a_n)$ onde cada $a_i \in K$. Assim,

$$K^n = \left\{ (a_1, \ldots, a_n) : \begin{matrix} a_i \in K \\ i = 1, \ldots, n \end{matrix} \right\}.$$

Dois elementos $(a_1, \ldots, a_n)$ e $(b_1, \ldots, b_n)$ de $K^n$ são iguais se $a_i = b_i$ $\forall i \in \{1, \ldots, n\}$.

Se definimos,

(1) $$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$
onde $(a_1, \ldots, a_n)$ e $(b_1, \ldots, b_n) \in K^n$.

(2) $$\lambda(a_1, \ldots, a_n) = (\lambda a_1, \ldots, \lambda a_n)$$
onde $\lambda \in K$ e $(a_1, \ldots, a_n) \in K^n$.

Segue imediatamente (verifique) que $K^n$ com as operações definidas acima é um espaço vetorial sobre o corpo $K$. Em particular $\mathbb{R}^n$ é um espaço vetorial sobre $\mathbb{R}$.

EXEMPLO 2. Sejam $S$ um conjunto não vazio e $K$ um corpo qualquer. Consideremos o conjunto $\mathscr{F}(S, K)$ de todas funções $f: S \to K$.

Sejam $f, g \in \mathscr{F}(S, K)$ e $\lambda \in K$. Definindo:

$$(f + g)(s) = f(s) + g(s) \quad \forall\, s \in S$$
$$(\lambda f)(s) = \lambda \cdot f(s) \quad \forall\, s \in S$$

também temos que $\mathscr{F}(S, K)$ é um espaço vetorial sobre o corpo $K$. Em particular $\mathscr{F}([0, 1], \mathbb{R})$ é um espaço vetorial sobre $\mathbb{R}$.

EXEMPLO 3. Sejam $K$ um corpo qualquer, $L \supset K$ uma extensão e $\alpha \in L$. Verifique que pode se definir operações sobre $K[x]$ (respectivamente $K[\alpha]$) de modo que $K[x]$ (respectivamente $K[\alpha]$ torna-se um espaço vetorial sobre $K$.

EXEMPLO 4. Finalmente $L \supset K$ é uma extensão de corpos $L$ pode ser visto como espaço vetorial sobre o corpo $K$. De fato, as operações

$$L \times L \to L \qquad \text{e } K \times L \to L$$
$$(u, v) \rightsquigarrow u + v) \qquad (\lambda, u) \rightsquigarrow \lambda u$$

já existem de modo natural no corpo $L$. A verificação das propriedades que definem espaço vetorial deixamos como exercício.

Até o fim desse parágrafo $K$ representa um corpo e $V$ um espaço vetorial sobre $K$.

Um subconjunto não vazio $W$ de $V$ diz-se um *subespaço vetorial de* $V$ se as seguintes condições são satisfeitas:

$$\text{SE}_1)\ w_1, w_2 \in W \Rightarrow w_1 + w_2 \in W$$
$$\text{SE}_2)\ \lambda \in K, w \in W \Rightarrow \lambda w \in W.$$

Observe que pelas condições acima as operações do espaço vetorial $V$ induzem operações em $W$ e $W$ é ele próprio um espaço vetorial com as operações induzidas.

Se $v_1, \ldots, v_n \in V$ dizemos que $v_1, \ldots, v_n$ são *linearmente independentes* se a equação vetorial $\sum_{i=1}^{n} \alpha_i v_i = 0, \alpha_i \in K$ é satisfeita apenas para os escalares $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$. Caso contrário dizemos que $v_1, \ldots, v_n$ são *linearmente dependentes.*

Usaremos simbolicamente L. I. para linearmente independentes e L. D. para linearmente dependentes. Por exemplo, $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 0, 1)$ são L. I. em $K^n$.

Se $u_1, u_2, \ldots, u_r \in V$ então é fácil verificar que

$$W = \left\{ \sum_{i=1}^{r} \alpha_i u_i : \alpha_i \in K, i = 1, \ldots, r \right\}$$

é um subespaço vetorial de $V$, o qual chamaremos de *subespaço gerado por* $u_1, \ldots, u_r$. Denotaremos esse espaço por,

$$W = \langle u_1, \ldots, u_r \rangle.$$

Se um conjunto (ordenado) $v_1, \ldots, v_n \in V$ for L. I. e tal que $\langle v_1, \ldots, v_n \rangle = V$ dizemos que $v_1, \ldots, v_n$ é uma base de $V$.
Por exemplo, $e_1, \ldots, e_n$ é uma base de $K^n$.

Agora vamos enunciar (sem demonstração) o seguinte teorema.

TEOREMA 2. (a) *Todo espaço vetorial $V$ sobre um corpo $K$ possui uma base.*

(b) *se um espaço vetorial $V$ sobre um corpo $K$ possui uma base com $n$ elementos então toda base de $V$ possui $n$ elementos.* ■

Se um espaço vetorial $V$ sobre um corpo $K$ possui uma base com $n$ elementos, chamamos ao número $n$ de *dimensão de $V$ sobre $K$* e denotamos $[V : K] = n$.

Observe que $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{R}$ de dimensão 2 pois $1, i \in \mathbb{C}$ é uma base desse espaço. Assim $[\mathbb{C} : \mathbb{R}] = 2$.

Agora vamos mostrar algumas proposições importantes no desenvolvimento da nossa teoria. Antes vamos dar a seguinte definição:

Seja $K$ um corpo qualquer. Uma extensão $L \supset K$ diz-se *finita* se $[L : K] = n < \infty$. Caso contrário $L \supset K$ diz-se uma *extensão infinita.*

PROPOSIÇÃO 3. *Seja $K$ um corpo e $L \supset K$ uma extensão de $K$. Então,*

(a) *se $L \supset K$ é finita então $L \supset K$ é algébrica.*

(b) *se $\alpha \in L \supset K$ é um elemento algébrico sobre $K$ e grau de irr$(\alpha, K)$ é igual a $n$ então $1, \alpha, \ldots, \alpha^{n-1}$ é uma base do espaço vetorial $K[\alpha]$ sobre $K$ e $[K[\alpha] : K] = n < \infty$.*

(c) *se $\alpha \in L \supset K$ é um elemento transcendente sobre $K$ então $K[\alpha] \supset K$ é uma extensão infinita.*

*Demonstração.* (a) seja $[L:K] = m < \infty$ e $\alpha \in L \supset K$ sendo $K[\alpha]$ um subespaço de $L$ segue imediatamente que $[K[\alpha]:K] \leq \leq m < \infty$. Se $[K[\alpha]:K] = n$ então $1, \alpha, \ldots, \alpha^n$ são L. D., pois $n$ é o número máximo de elementos L. I., e portanto existem escalares $a_0, a_1, \ldots, a_n$ não todos nulos tais que

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$$

e isso nos diz que $\alpha$ é algébrico sobre $K$.

(b) seja $\alpha \in L \supset K$ um elemento algébrico sobre $K$ tal que grau de irr(($\alpha$, $K$) = $n$.

Vimos pela Proposição 1 deste capítulo que todo elemento de $K[\alpha]$ pode ser escrito de modo único como combinação linear sobre $K$ de $1, \alpha, \ldots, \alpha^{n-1}$. Assim $1, \alpha, \ldots, \alpha^{n-1}$ é uma base de $K[\alpha]$ sobre $K$ e isto nos diz que $[K[\alpha]:K] = n$.

(c) Decorre imediatamente do item (a). ■

O seguinte corolário decorre imediatamente da Proposição 3.

COROLÁRIO 1. *Seja $\alpha \in L \supset K$. Então as seguintes afirmações são equivalentes:*

(i) *$\alpha$ é algébrico sobre $K$*

(ii) $[K[\alpha]:K] < \infty$

(iii) *$K[\alpha]$ é uma extensão algébrica de $K$.*

PROPOSIÇÃO 4. *Sejam $M \supset L \supset K$ corpos tais que $[M:L]$ e $[L:K]$ são finitos então $[M:K]$ é finito e*

$$[M:K] = [M:L] \cdot [L:K].$$

*Demonstração.* Seja $v_1, \ldots, v_r$ uma base de $M$ sobre $L$ e seja $u_1, \ldots, u_s$ uma base de $L$ sobre $K$. Vamos provar que:

$$\beta = \left\{ v_i \cdot u_j : \begin{matrix} i = 1, \ldots, r \\ j = 1, \ldots, s \end{matrix} \right\}$$

é uma base de $M$ sobre $K$ e isto demonstra a proposição.

De fato, primeiramente vamos provar que $\beta$ é um conjunto L.I. em $M$ sobre $K$.

Se $\alpha_{ij} \in K, 1 \leq i \leq r, 1 \leq j \leq s$, e $\sum_{i,j} \alpha_{ij} v_i u_j = 0$.

Podemos reescrever essa equação do seguinte modo:

$(\alpha_{11}u_1 + \alpha_{12}u_2 + \ldots + \alpha_{1s}u_s)v_1 + \ldots + (\alpha_{r1}u_1 + \alpha_{r2}u_2 + \ldots + \alpha r_s u_s)v_r = 0.$

Ora como os $u_j's$ estão em $L$ segue, pela independência linear dos $v_i's$ em $M$ sobre $L$, que:

$$\begin{cases} \alpha_{11}u_1 + \alpha_{12}u_2 + \dots + \alpha_{1s}u_s = 0 \\ \vdots \\ \alpha_{r1}u_1 + \alpha_{r2}u_2 + \dots + \alpha_{rs}u_s = 0 \end{cases}$$

Agora como os $\alpha_{ij}'s$ estão em $K$ segue pela independência linear dos $u_j's$ em $L$ sobre $K$ que cada $\alpha_{ij} = 0, 1 \leq i \leq r, 1 \leq j \leq s$. Assim $\beta$ é um conjunto L. I. de $M$ sobre $K$.

Agora vamos provar que $\beta$ é um conjunto gerador de $M$ sobre $K$. De fato, seja $y \in M$.

Sendo $v_1, \dots, v_r$ uma base de $M$ sobre $L$ existem $\lambda_1, \dots, \lambda_r \in L$ tais que,

$$y = \lambda_1 v_1 + \dots + \lambda_r v_r.$$

Sendo cada $\lambda_i \in L$ e $u_1, u_2, \dots, u_s$ uma base de $L$ sobre $K$ existem $\alpha_{ij} \in K, 1 \leq i \leq r, 1 \leq j \leq s$ tais que,

$$\lambda_i = \alpha_{i1}u_1 + \alpha_{12}u_2 + \dots + \alpha_{is}u_s.$$

Daí segue imediatamente que,

$$y = \sum_{i,j} \alpha_{ij} v_i u_j, \alpha_{ij} \in K, \ 1 \leq i \leq r, \ 1 \leq j \leq s,$$

como queríamos demonstrar. ■

**COROLÁRIO 1.** (a) $\bar{\mathbb{Q}}_{\mathbb{C}} = \{\alpha \in \mathbb{C} : \alpha$ *algébrico sobre* $\mathbb{Q}\}$ *é um subcorpo de* $\mathbb{C}$, *que é uma extensão algébrica infinita de* $\mathbb{Q}$.

(b) $\bar{\mathbb{Q}}_{\mathbb{R}} = \{\alpha \in \mathbb{R} : \alpha$ *algébrico sobre* $\mathbb{Q}\}$ *é um subcorpo de* $\mathbb{R}$, *que é uma extensão algébrica infinita de* $\mathbb{Q}$.

*Demonstração.* (a) Claramente o subconjunto $\bar{\mathbb{Q}}_{\mathbb{C}}$ de $\mathbb{C}$ contém $\mathbb{Q}$. Para provarmos que $\bar{\mathbb{Q}}_{\mathbb{C}}$ é um subcorpo de $\mathbb{C}$ é suficiente provarmos as seguintes três propriedades:

1) $\alpha, \beta \in \bar{\mathbb{Q}}_{\mathbb{C}} \Rightarrow \alpha - \beta \in \bar{\mathbb{Q}}_{\mathbb{C}}$

2) $\alpha, \beta \in \bar{\mathbb{Q}}_{\mathbb{C}} \Rightarrow \alpha \cdot \beta \in \bar{\mathbb{Q}}_{\mathbb{C}}$

3) $0 \neq \alpha \in \bar{\mathbb{Q}}_{\mathbb{C}} \Rightarrow \alpha^{-1} = \dfrac{1}{\alpha} \in \bar{\mathbb{Q}}_{\mathbb{C}}$.

Vamos demonstrar simultaneamente 1), 2) e 3). De fato,

Seja $K = \mathbb{Q}[\alpha]$ e $L = K[\beta]$. Como $\alpha$ é algébrico sobre $\mathbb{Q}$ segue que $[K : \mathbb{Q}] < \infty$. Agora claramente sendo $\beta$ algébrico sobre $\mathbb{Q}$, $\beta$ também é algébrico sobre $K$ e daí segue que $[L : K] < \infty$.

Pela proposição anterior temos que,

$$[L:\mathbb{Q}] = [L:K]\cdot[K:\mathbb{Q}] < \infty$$

e pela Proposição 3 temos $L \supset \mathbb{Q}$ é uma extensão algébrica. Agora o resultado sai imediatamente pois $\alpha \pm \beta \in L, \alpha\cdot\beta \in L$ e $\frac{1}{\alpha} \in L$ se $\alpha \neq 0$.
Imediatamente segue que $\bar{\mathbb{Q}}_{\mathbb{C}}$ é uma extensão algébrica sobre $\mathbb{Q}$. Agora se $\alpha_i = \sqrt[2^i]{2}$ e $K_0 = \mathbb{Q}$, $K_1 = \mathbb{Q}[\alpha_1], \ldots, K_i = K_{i-1}[\alpha_i]$ temos que $M = \bigcup_{i=0}^{\infty} K_i$ é uma extensão algébrica infinita de $\mathbb{Q}$ e $M \subset \bar{\mathbb{Q}}_{\mathbb{R}} \subset \bar{\mathbb{Q}}_{\mathbb{C}}$.

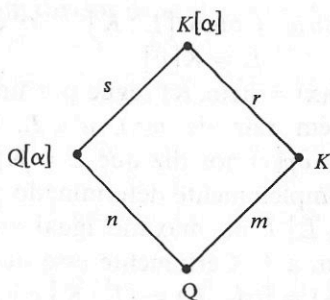
(b) Basta observar que $\bar{\mathbb{Q}}_{\mathbb{R}} = \bar{\mathbb{Q}}_{\mathbb{C}} \cap \mathbb{R}$ e também

$$M = \bigcup_{i=0}^{\infty} K_i \subset \bar{\mathbb{Q}}_{\mathbb{R}}. \blacksquare$$

COROLÁRIO 2. *Seja $K \supset \mathbb{Q}$ tal que $[K:\mathbb{Q}] = m$ e seja $p(x) \in \mathbb{Q}[x]$ um polinômio irredutível sobre $\mathbb{Q}$ de grau $n$.*

*Se M.D.C. $\{m, n\} = 1$ então $p(x)$ é um polinômio irredutível sobre $K$.*

*Demonstração.* Seja $\alpha \in \mathbb{C}$ uma raiz de $p(x)$. Considere agora os corpos $\mathbb{Q}[\alpha] \subset K[\alpha]$ e suponhamos que $[K[\alpha]:K] = r$ e $[K[\alpha]:\mathbb{Q}[\alpha]] = s$.

Claramente temos $[\mathbb{Q}[\alpha]:\mathbb{Q}] = n$ e $[K[\alpha]:K] = r = n$. De fato, pela Proposição 6 (veja figura abaixo) segue que

$n\cdot s = m\cdot r$ e como M.D.C. $\{n, m\} = 1$ vem $n \backslash r$. Mas $r \leq n$ nos diz que $n = r$ e assim $p(x)$ é também irredutível sobre $K$. $\blacksquare$

COROLÁRIO 3. *Seja $L = Gal(x^p - 2, \mathbb{Q})$. Então $[L:\mathbb{Q}] = p.(p-1)$.*

*Demonstração.* De fato, sabemos que $L = \mathrm{Gal}(x^p - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, u]$ onde $\alpha = \sqrt[p]{2} \in \mathbb{R}$ e $u = \left(\cos\frac{2\pi}{p} + i \operatorname{sen}\frac{2\pi}{p}\right) \in \mathbb{C}$ é uma raiz p-ésima da unidade tal que $1, u, u^2, \ldots, u^{p-1}$ nos dão todas as distintas raízes p-ésimas da unidade em $\mathbb{C}$ (por isso $u$ diz-se ser uma *raiz primitiva da unidade).*

Agora pela Proposição 6,

$$[L : \mathbb{Q}] = [L : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}].$$

Pelo critério de Eisenstein temos $[\mathbb{Q}[\alpha] : \mathbb{Q}] = p$. Agora se $K = \mathbb{Q}[\alpha]$ temos $L = K[u] \supset K \supset \mathbb{Q}$. Ainda por Eisenstein temos que $u$ é raiz de $x^{p-1} + x^{p-2} + \ldots + x + 1$ que é polinômio irredutível de grau $p - 1$ sobre $\mathbb{Q}$. Como $[K : \mathbb{Q}] = p$ e M.D.C. $\{p, p-1\} = 1$ temos pelo corolário anterior que $x^{p-1} + x^{p-2} + \ldots + x + 1$ é ainda irredutível sobre $K$ tendo $u$ como raiz. Portanto $[K[u] : K] = p - 1$ e isto demonstra o nosso corolário pois

$$L = K[u] \text{ e } K = \mathbb{Q}[\alpha]. \blacksquare$$

TEOREMA 3. *Seja $L \supset K \supset \mathbb{Q}$ tal que $[L : K] < \infty$. Então, $\exists\, u \in L$ tal que $L = K[u]$.*

COROLÁRIO 1. *Seja $L \supset K \supset \mathbb{Q}$ tal que $[L : K] < \infty$. Então, $[L : K] \geq |\mathrm{Aut}_K L|$ (onde $|\mathrm{Aut}_K L|$ denota o número de elementos do conjunto $\mathrm{Aut}_K L = \{f \in \mathrm{Aut}\ L : f(\lambda) = \lambda\ \forall\, \lambda \in K\}$).*

*Demonstração do Corolário.* Como $[L : K] < \infty$ existe $u \in L$ tal que $L = K[u]$.

Agora se $\sigma \in \mathrm{Aut}_K L$ e $p(x) = \mathrm{irr}(u, K)$ segue por um exercício anterior que $u' = \sigma(u)$ é também raiz de $p(x)$, $u' \in L$. Ora $K[u'] \subset L$ e $[K[u'] : K] = [L : K] = \partial p(x)$ nos diz que $L = K[u] = K[u']$. Como $\sigma(a) = a\ \forall\, a \in K\ \sigma$ fica completamente determinado pelo valor $u' = \sigma(u)$. Assim o número $|\mathrm{Aut}_K L|$ é no máximo igual ao número de raízes $u'$ de $p(x)$ que pertencem a $L$. Certamente esse número é no máximo o grau do polinômio $p(x) = \mathrm{irr}(u, K) = [L : K]$ e isto demonstra nosso corolário. $\blacksquare$

*Demonstração do Teorema* 3. A demonstração será por indução sobre o grau $[L : \mathrm{K}] < \infty$.

Se $[L : K] = 1$ segue que $L = K$ e o teorema é válido trivialmente.

Suponhamos $[L:K] > 1$. Assim $\exists\, \alpha_1 \in L$, $\alpha_1 \notin K$.

Seja $K_1 = K[\alpha_1]$. Se $K_1 = L$ o teorema está demonstrado. Assim, $\exists\, \alpha_2 \in L$ tal que $\alpha_2 \notin K_1$.

Seja $K_2 = K_1[\alpha_2] = K[\alpha_1; \alpha_2]$. Como $[L:K] < \infty$ conseguimos $\alpha_1, \alpha_2, \ldots, \alpha_r$, $r \geq 2$, elementos de $L$ tais que, $L = K[\alpha_1, \alpha_2, \ldots, \alpha_r]$ e $\alpha_i \notin K[\alpha_1, \ldots, \alpha_{i-1}] = K_{i-1}$, $K_r = L \supseteq K_{r-1} =$ $= K[\alpha_1, \ldots, \alpha_{r-1}] \supset \ldots \supset K_1 = K[\alpha_1] \supset K_0 = K$.
Como $[K_{r-1} : K] < \infty$ temos pela hipótese de indução que $\exists\, \alpha \in K_{r-1}$ tal que $K_{r-1} = K[\alpha]$ e daí segue imediatamente que $L = K_r = K[\alpha, \alpha_r]$.
Chamando $\alpha_r = \beta \in L$ temos $L = K[\alpha, \beta]$.
Agora vamos provar que existe $u \in L$ tal que $L = K[u]$.

Sejam $p(x) = \operatorname{irr}(\alpha, K)$ e $q(x) = \operatorname{irr}(\beta, K)$ tais que $\partial p(x) = m$ e $\partial q(x) = n$. Pela proposição 2, item b deste capítulo segue que todas as raízes de $p(x)$ (respectivamente de $q(x)$) são distintas em $\mathbb{C}$.
Sejam $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ as raízes de $p(x)$ em $\mathbb{C}$ e sejam $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ as raízes de $q(x)$ em $\mathbb{C}$. Vamos definir para $j \neq 1$ os seguintes números complexos,

$$j \neq 1,\ \lambda_{ij} = \frac{\alpha_i - \alpha}{\beta - \beta_j} \in \mathbb{C}.$$

Como $K$ é um corpo infinito então $\exists\, \lambda \in K$ tal que $\lambda \notin \left\{ \lambda_{ij} : \begin{matrix} 1 \leq i \leq m \\ 2 \leq j \leq n \end{matrix} \right\}$.
Agora seja $u = \alpha + \lambda\beta \in L$ e assim $K[u] \subset L$, vamos provar que de fato $L = K[u]$. Para isso vamos provar que $\alpha, \beta \in K[u]$.

Seja $F = K[u]$ e seja $h(x) = p(u - \lambda x) \in F[x]$, observe que $h(\beta) =$ $= p(u - \lambda\beta) = p(\alpha) = 0$. Mas $\beta$ também é raiz de $q(x) \in K[x] \subset F[x]$.
Portanto $(x - \beta)$ é um divisor de $d(x) = \text{M.D.C.}_{\mathbb{C}[x]}\,\{q(x), h(x)\}$. Vamos de fato provar que $d(x) = x - \beta$, e para isso é suficiente provarmos que se $d(\beta_j) = 0$ então $j = 1$ já que $d(x) \backslash q(x)$, e $q(x)$ só possui raízes simples.

Se $d(\beta_j) = 0$ e $j \neq 1$ teremos $h(\beta_j) = 0$ ou seja $p(u - \lambda\beta_j) = 0$ o que nos diz que $\exists\, i$, $1 \leq i \leq m$ tal que $\alpha_i = u - \lambda\beta_j = \alpha + \lambda\beta - \lambda\beta_j$ e daí segue que $\lambda = \lambda_{ij}$ contradizendo a nossa escolha de $\lambda$. Portanto $x - \beta = d(x)$.

Agora se $d_1(x) = \text{M.D.C.}_{F[x]}\,\{q(x), h(x)\}$ temos por $F \subset \mathbb{C}$ que grau $d_1(x) \leq$ grau $d(x)$. Portanto se $d_1(x) \neq d(x)$ teríamos que $1 =$ $= \text{M.D.C.}_{F[x]}\,\{q(x), h(x)\}$ mas então seguiria (prove isto) que $d(x) = 1$ o que é absurdo. Logo $d(x) = x - \beta = \text{M.D.C.}_{F[x]}\,\{q(x), h(x)\}$ e isto nos diz que $\beta \in F$. Agora, $\alpha = u - \lambda\beta \in F$ pois $u \in F = K[u]$, $\beta \in F$, $\lambda \in K \subset F$ e isto demonstra o Teorema 4. ■

Terminaremos esse parágrafo fazendo algumas observações.

Uma extensão $L \supset K$ diz-se *simples* se $\exists\, u \in L$ tal que $L = K[u]$. O Teorema 3 que acabamos de demonstrar nos diz que "toda extensão finita $L \supset K$ de característica zero é simples". Esse teorema nos será bastante útil no Capítulo 7 quando desenvolveremos a Teoria de Galois sobre um corpo de característica zero. Por exemplo, com a ajuda do Teorema 3 provaremos que se $L = \mathrm{Gal}(f, K)$ onde $K$ é um corpo de característica zero então $[L:K] = |\mathrm{Aut}_K L|$ (observe que no Corolário 1 do Teorema 3 nós provamos que em geral, se $L \supset K \supset \mathbb{Q}$ vale a desigualdade

$$[L:K] \geq |\mathrm{Aut}_K L|).$$

No próximo capítulo provaremos que $\mathrm{Aut}_K\, L$ é mais que um conjunto, ele possui a estrutura de um grupo com a operação composição de funções.

## EXERCÍCIOS

1. Complete todas as afirmações deixadas sem demonstração, inclusive a demonstração do Teorema 3.

2. Seja $K$ um corpo e $V$ um espaço vetorial sobre $K$. Se $v_1, \ldots, v_n \in V$, prove que:

   $v_1, \ldots, v_n$ é uma base de $V \Leftrightarrow$ Todo elemento de $V$ pode ser escrito de modo único como combinação linear sobre $K$ de $v_1, \ldots, v_n$

   $\left[\sum_{i=1}^{n} \alpha_i v_i\right.$ diz-se uma *combinação linear sobre* $K$ se $\left.\alpha_i \in K, i = 1, \ldots, n\right]$

3. Seja $K$ um corpo e $V$ um espaço vetorial sobre $K$. Um subconjunto infinito $\beta$ de $V$ diz-se L. I. se toda parte finita de $\beta$ é L. I. Prove que:

   $\{1, x, x^2, \ldots, x^n, \ldots\}$ é um conjunto L. I. no espaço vetorial $K[x]$ sobre $K$.

4. Seja $K$ um corpo e $V$ um espaço vetorial sobre $K$. Se $\beta$ é um conjunto infinito definimos

   $$\langle\beta\rangle = \left\{\sum_{i=1}^{n} \alpha_i v_i : \begin{matrix} \alpha_i \in K, v_i \in \beta \\ i = 1, \ldots, n \end{matrix}, n \in \mathbb{N}\right\}, \text{ isto é,}$$

   $\langle\beta\rangle$ é o conjunto de todas as combinações lineares finitas sobre $K$ de elementos de $\beta$.

Prove que:

(a) $\langle \beta \rangle$ é um subespaço vetorial de $V$

(b) se $\beta = \{1, x, x^2, \ldots, x^n, \ldots\}$ então $\langle \beta \rangle = K[x]$.

5. Seja $K$ um corpo e $V$ um espaço vetorial sobre $K$. Um conjunto (não necessariamente finito) $\beta \subset V$ diz-se uma base de $V$ se $\beta$ é L. I. e $\langle \beta \rangle = V$.

   Prove que:

   (a) $\beta = \{1, x, \ldots, x^n, \ldots\}$ é uma base de $K[x]$
   (Nesse caso dizemos que $[K[x] : K] = \infty$)

   (b) Se $\alpha \in L \supset K$ é transcendente sobre $K$ então $\{1, \alpha, \alpha^2, \ldots, \alpha^n, \ldots\}$ é uma base de $K[\alpha]$ sobre $K$.

6. Seja $K$ um corpo e $V$ um espaço vetorial sobre $K$. Um conjunto $\beta \subset V$ diz-se *maximal L. I. em* $V$ se $\beta$ é L. I. e se $v \in V, v \notin \beta$ então $\beta \cup \{v\}$ é L. D. em $V$. Um conjunto $\beta \subset V$ diz-se *maximal gerador em* $V$ se $\langle \beta \rangle = V$ e $\forall u \in \beta \ \langle \beta - \{u\} \rangle \neq V$.

   Prove que se $\beta$ é um subconjunto de $V$ então as seguintes condições são equivalentes:

   (a) $\beta$ é uma base de $V$

   (b) $\beta$ é um conjunto maximal L. I.

   (c) $\beta$ é um conjunto maximal gerador.

7. Seja $K$ um corpo e $V$ um espaço vetorial de dimensão $[V : K]$ finita. Prove que:

   (a) Todo subconjunto L.I. de $V$ pode ser extendido para uma base de $V$.

   (b) De todo subconjunto finito gerador de $V$ podemos extrair uma base de $V$.

   (c) Se $W$ é um subespaço de $V$ e $W \neq V$ então $[W : K] < [V : K]$.

8. (a) Defina homorfismos e isomorfismos de espaços vetoriais sobre um mesmo corpo $K$.

   (b) Prove que: se $K^n$ é isomorfo a $K^m$ então $m = n$.

9. Seja $K$ um corpo e $V$ e $V'$ espaços vetoriais sobre $K$. Prove que: se $v_1, \ldots, v_n$ é uma base de $V$ e $u'_1, \ldots, u'_n$ são elementos quaisquer de $V'$ então existe um único homomorfismo $T : V \rightarrow V'$ tal que $T(v_i) = u'_i$, $i = 1, \ldots, n$.

10. Seja $K$ um corpo e $V$ um espaço vetorial sobre o corpo $K$. Se $W$ é um subespaço vetorial de $V$ defina o *espaço vetorial quociente* $V/W$. Prove que:
    se $[V : K]$ finita então $[V/W : K] = [V : K] - [W : K]$.

11. Seja $K$ um corpo e $V$ e $V'$ espaços vetoriais sobre $K$. Se $T: V \to V'$ é um homomorfismo então
    (a) $\operatorname{Im} T = \{T(v) : v \in V\}$ é um subespaço vetorial de $V'$, e mais $T$ é sobrejetiva $\Leftrightarrow \operatorname{Im}(T) = V'$
    (b) $N(T) = \{v \in V : T(v) = 0' =$ elemento neutro de $V'\}$ é um subespaço vetorial de $V$, e mais $T$ é injetiva $\Leftrightarrow N(T) = \{0\}$.
    (c) $V/N(T)$ é isomorfo a $\operatorname{Im}(T)$ [e daí segue como corolário que $[V : K] = [\operatorname{Im}(T) : K] + [N(T) : K]$].

12. Sejam $K$ e $L$ corpos e seja $0 \neq \alpha \in L \supset K$. Se $f(x) \in K[x]$ é tal que $f(\alpha) = 0$, calcule um polinômio $g(x) \in K[x]$ tal que $g\left(\frac{1}{\alpha}\right) = 0$.

13. Seja $K$ um corpo e $L \supset K$ uma extensão de $K$. Se $\alpha \in L$. Prove que:
    (a) $\alpha$ é algébrico sobre $K \Leftrightarrow [K[\alpha] : K] < \infty$
    (b) $\alpha$ é transcendente sobre $K \Leftrightarrow [K[\alpha] : K] = \infty$.

14. Calcule $[L : Q]$ para as seguintes extensões $L \supset \mathbb{Q}$.
    (a) $L = \operatorname{Gal}(x^4 - 2, \mathbb{Q})$; (b) $L = \operatorname{Gal}(x^5 - 3, \mathbb{Q})$;
    (c) $L = \operatorname{Gal}(x^6 - 2, \mathbb{Q})$; (d) $L = \operatorname{Gal}(x^7 - 2, \mathbb{Q})$;
    (e) $L = \operatorname{Gal}(x^8 - 2, \mathbb{Q})$.

15. Achar $u \in \mathbb{Q}[\alpha, \beta] = L$ de modo que $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[u]$:
    (a) $\alpha = \sqrt{2}$, $\beta = i$; (b) $\alpha = \sqrt{2}$, $\beta = \sqrt[3]{2}$;
    (c) $\alpha = \sqrt[3]{5}$, $\beta = \sqrt{-2}$; (d) $\alpha = \sqrt{8}$, $\beta = 3 + \sqrt{50}$;
    (e) $\alpha = \sqrt[3]{2}$, $\beta$ é tal que $\beta^4 + 6\beta + 2 = 0$.

16. Em cada item do exercício anterior, calcular $[\mathbb{Q}[\alpha, \beta] : \mathbb{Q}]$?

17. Seja $L = K[\alpha_1, \ldots, \alpha_r]$ onde cada $\alpha_i \in \mathbb{C}$ é algébrico sobre $K_{i-1} = K[\alpha_1, \ldots, \alpha_{i-1}]$ então $L$ é um corpo e $L \supset K$ é uma extensão finita.

18. Seja $p(x)$ um polinômio de grau ímpar irredutível sobre o corpo $K \supset \mathbb{Q}$ e se $L \supset K$ é uma extensão finita de grau potência de 2, então $p(x)$ é ainda irredutível sobre $L$.

19. Responda se os seguintes polinômios $f(x) \in K[x]$ são irredutíveis sobre $K$:
    (a) $f(x) = x^2 + 3$; $K = \mathbb{Q}[\sqrt{5}]$
    (b) $f(x) = x^3 + 8x - 2$; $K = \mathbb{Q}[\sqrt{2}]$
    (c) $f(x) = x^5 + 3x^3 - 9x - 6$; $K = \mathbb{Q}[\sqrt{7}, \sqrt{5}, i]$

20. Se $\alpha = \pi^6 + 5\pi^3 - 1$ responda se $\alpha$ é algébrico ou transcendente (sobre $\mathbb{Q}$).

21. Calcular $\cos 3\theta$ em função de $\cos\theta$.

22. Seja $K$ um corpo qualquer e $L \supset K$ tal que $[L:K] = p$ é um número primo.
Prove que:
$$L = K[u]\ \forall\, u \in L, u \notin K.$$

23. Prove que não existe elemento $u \in \mathbb{Q}(x)$ tal que $u^2 = x$.

24. Seja $K$ um corpo e $L \supset K$ uma extensão. Um elemento $\alpha \in L$ algébrico sobre $K$ diz-se *separável sobre* $K$ se $\exists\, f(x) \in K[x]$ tal que $f(\alpha) = 0$ e $f(x)$ não possui raízes múltiplas em nenhuma extensão de $K$.
$L \supset K$ diz-se *separável sobre* $K$ se todos os elementos de $L$ são separáveis sobre $K$.
Um corpo $K$ diz-se *perfeito* se todas as extensões finitas de $K$ são separáveis.
Prove que:
Todo corpo de característica zero é perfeito.

25. Seja $L \supset K$ uma extensão finita.
Prove que:
Se $L \supset K$ é separável então $L = K[u]$ é uma extensão simples (Sugestão: veja a demonstração do Teorema 4).

26. Se $L \supset K$ é uma extensão e $\alpha, \beta \in L$ são tais que, $\alpha$ ou $\beta$ é separável sobre $K$ então $K[\alpha, \beta] = K[u]$ é uma extensão simples.

27. Se $K = K_0 \subset K_1 \subset \ldots \subset K_r = L$ são corpos e $[L:K] < \infty$ temos,
$$[L:K] = [K_r : K_{r-1}] \ldots [K_2 : K_1] \cdot [K_1 : K_0].$$

28. Seja $K$ um corpo qualquer e $L \supset K$ uma extensão de $K$. Se $f(x)$, $g(x) \in K[x]$ então, prove que,
(a) $\text{M.D.C.}_{L[x]}\ \{f(x),\ g(x)\} = 1 \Leftrightarrow \exists\ a(x),\ b(x) \in L[x]$ tais que $a(x)\cdot f(x) + b(x)\cdot g(x) = 1$.
(b) $\text{M.D.C.}_{K[x]}\ \{f(x), g(x)\} = 1 \Leftrightarrow \text{M.D.C.}_{L[x]}\ \{f(x), g(x)\} = 1$.

## §4 Construção por meio de régua e compasso

Neste parágrafo mostraremos a impossibilidade de construções com o uso apenas dos instrumentos régua e compasso. Aqui, a régua

considerada não possui qualquer marca, é apenas um instrumento que nos permite ligar dos pontos do plano $\mathbb{R}^2$.

Veremos os problemas clássicos da duplicação do cubo e da trissecção do ângulo. Convém observar que se admitirmos uma régua com marcas indicando segmentos de um certo comprimento, então é possível trissectar um ângulo [veja a construção feita no Exemplo 1].

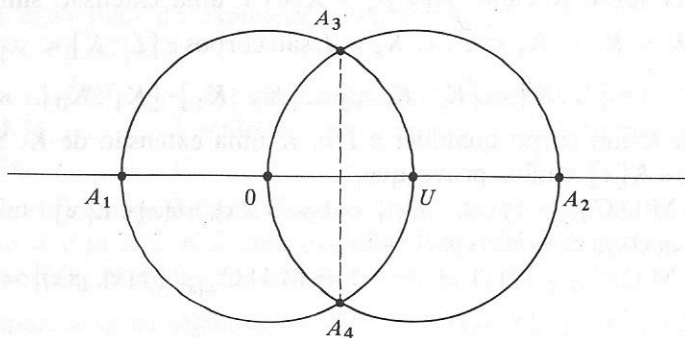
Seja $\mathscr{P}$ um subconjunto do $\mathbb{R}^2$ contendo pelo menos dois pontos distintos. Dizemos que uma reta $r$ de $\mathbb{R}^2$ é *uma reta em* $\mathscr{P}$ se $r$ contém dois distintos pontos de $\mathscr{P}$, e dizemos que uma circunferência $c$ em $\mathbb{R}^2$ é *uma circunferência em* $\mathscr{P}$ se o centro de $c$ pertence a $\mathscr{P}$ e um ponto de $\mathscr{P}$ pertence a $c$.

Chamaremos (I), (II), (III) abaixo, de *operações elementares em* $\mathscr{P}$:

(I) Interseção de duas retas em $\mathscr{P}$.
(II) Interseção de uma reta em $\mathscr{P}$ e uma circunferência em $\mathscr{P}$.
(III) Interseção de duas circunferências em $\mathscr{P}$.

Um ponto $A \in \mathbb{R}^2$ diz-se *construtível a partir de* $\mathscr{P}$ se podemos determinar $A$ através de uma dessas operações elementares em $\mathscr{P}$. Denotaremos por $\langle \mathscr{P} \rangle$ o subconjunto dos pontos de $\mathbb{R}^2$ que são construtíveis a partir de $\mathscr{P}$.

Por exemplo,

Se $\mathscr{P}_0 = \{0, U\}$ onde $0 = (0, 0)$ e $U = (1, 0)$ então, $\langle \mathscr{P}_0 \rangle = \{0, U, A_1, A_2, A_3, A_4\}$, como na figura abaixo, onde $A_1 = (-1,0)$, $A_2 = (2, 0)$, $A_3 = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$, $A_4 = \left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$.

Nesse parágrafo consideraremos sempre $0 = (0, 0)$ e $U = (1, 0)$.

Agora, seja $\mathscr{P}_0 = \{0, U\}$, $\mathscr{P}_1 = \langle \mathscr{P}_0 \rangle$ $\mathscr{P}_2 = \langle \mathscr{P}_1 \rangle, \ldots, \mathscr{P}_{n+1} = \langle \mathscr{P}_n \rangle$, $\forall n \in \mathbb{N}$.

Assim temos,

$$\mathscr{P}_0 \subset \mathscr{P}_1 \subset \mathscr{P}_2 \subset \dots \subset \mathscr{P}_n \subset \mathscr{P}_{n+1} \subset \dots \subset \mathbb{R}^2.$$

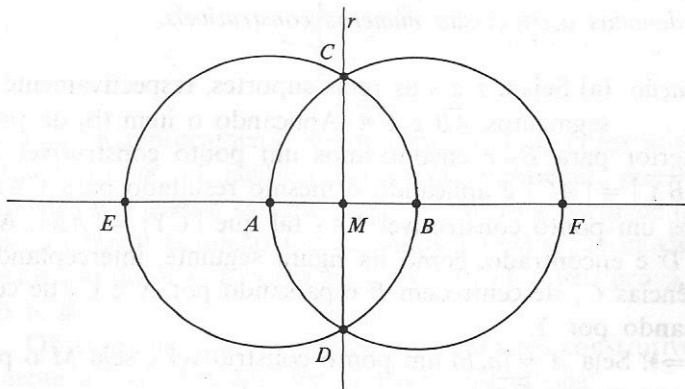
Seja $\mathscr{P}_\infty = \bigcup_{n=0}^{\infty} \mathscr{P}_n$. Claramente temos que $\mathscr{P}_\infty$ é um conjunto infinito embora cada $\mathscr{P}_n$ seja um subconjunto finito do $\mathbb{R}^2$. É imediato também que $\langle \mathscr{P}_\infty \rangle = \mathscr{P}_\infty$ e $(m, v) \in \mathscr{P}_\infty \ \forall m \in \mathbb{Z}, \forall v \in \mathbb{Z}$.

Os pontos do plano que pertencem a $\mathscr{P}_\infty$ são chamados de *pontos construtíveis* e as retas em $\mathscr{P}_\infty$, isto é, contendo dois distintos pontos construtíveis, são chamadas de *retas construtíveis*. Um número real $a$ diz-se *construtível* se $(a, 0) \in \mathscr{P}_\infty$.

PROPOSIÇÃO 5. (a) *Se $A$ e $B$ são distintos pontos construtíveis então o ponto médio $M$ do segmento $\overline{AB}$ é construtível e as retas perpendiculares a $\overline{AB}$ passando pelos pontos $A$, $B$ e $M$ também são construtíveis.*

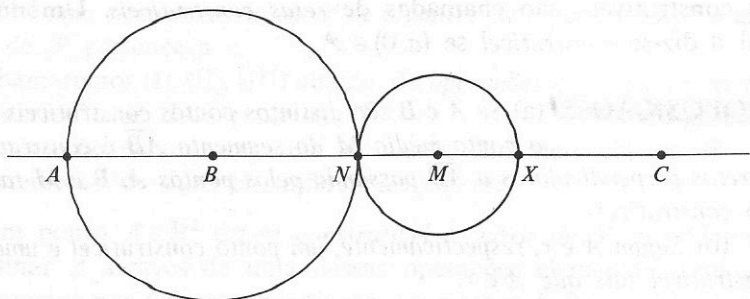
(b) *Sejam $A$ e $r$, respectivamente, um ponto construtível e uma reta construtível tais que $A \in r$.*

*Se $B$ e $C$ são pontos construtíveis então existe um ponto construtível $X$ tal que $X \in r$ e os segmentos $\overline{AX}$ e $\overline{BC}$ possuem o mesmo comprimento.*

*Demonstração.* (a) Usando duas circunferências centradas em cada um dos pontos e passando pelo outro, como na figura abaixo, fica provado o item (a) pois os pontos $C$, $D$, $E$, $F$ são construtíveis e mais ainda $A$ é o ponto médio de $\overline{EB}$ e $B$ é o ponto médio de $\overline{AF}$.

(b) Usando circunferências centradas em $B$ e centradas em $A$ podemos assumir que $A, B$ e $C$ pertencem a reta $r$.

Agora, seja $M$ o ponto médio de $BC$ e $N \in r$ um ponto construtível tal que $|\overline{AB}| = |\overline{BN}|$ (isto é, os segmentos $\overline{AB}$ e $\overline{BN}$ possuem o mesmo comprimento).

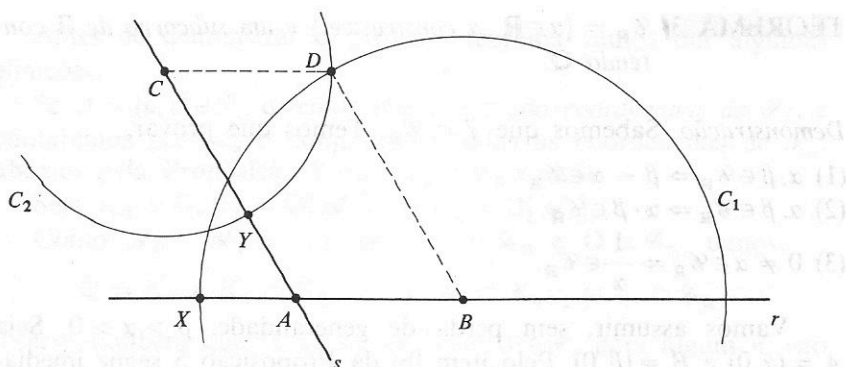
Assim, $A, B, C, M, N \in r$ são pontos construtíveis.

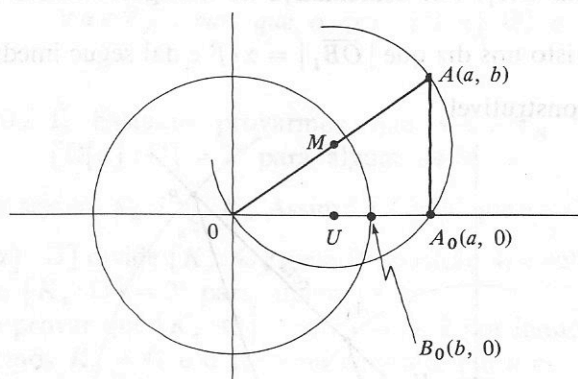
Seja $X \in r$ o ponto construtível, como na figura abaixo, tal que $|\overline{NM}| = |\overline{MX}|$.

Segue imediatamente da nossa construção que $|\overline{AB}| = |\overline{BN}| = |\overline{XC}|$ e portanto $|\overline{AX}| = |\overline{BC}|$, como queríamos demonstrar. ∎

PROPOSIÇÃO 6. (a) *Sejam $A$, $B$ e $C$ 3 pontos construtíveis não alinhados. Então existe um ponto construtível $D$ tal que $A$, $B$, $C$ e $D$ formam um paralelogramo. Em particular a reta passando por $C$ e paralela ao segmento $\overline{AB}$ é construtível.*

(b) *Um ponto $A = (a, b) \in \mathbb{R}^2$ é construtível se e somente se as suas coordenadas $a, b \in \mathbb{R}$ são números construtíveis.*

*Demonstração.* (a) Sejam $r$ e $s$ as retas suportes, respectivamente, dos segmentos $\overline{AB}$ e $\overline{CA}$. Aplicando o item (b) da proposição anterior para $B \in r$ encontramos um ponto construtível $X \in r$ tal que $|\overline{BX}| = |\overline{AC}|$ e aplicando o mesmo resultado para $C \in s$ encontramos um ponto construtível $Y \in s$ tal que $|\overline{CY}| = |\overline{AB}|$. Agora o ponto $D$ é encontrado, como na figura seguinte, interceptando as circunferências $C_1$ de centro em $B$ e passando por $X$ e $C_2$ de centro $C$ e passando por $Y$.

(b) $(\Rightarrow)$: Seja $A = (a, b)$ um ponto construtível e seja $M$ o ponto médio do segmento $\overline{OA}$.

Segue imediatamente da geometria elementar que o ponto $A_0 = (a,0)$ é a interseção a reta $\overline{OU}$ e da circunferência $C$ de centro $M$ passando por $A$ como na figura abaixo.

Achado o ponto $A_0 = (a, 0)$ pertencente a reta $\overline{OU}$ podemos pelo item (b) da proposição anterior encontrar o ponto $B_0 = (b, 0)$ traçando a partir de 0 uma circunferência de raio $|\overline{A_0 A}|$.

($\Leftarrow$): Reciprocamente suponhamos $a$ e $b$ construtíveis, isto é, $(a, 0)$ e $(b, 0) \in \mathscr{P}_\infty$. É fácil ver que a reta determinada por 0 e por $(0, 1)$ é construtível. Assim sabemos construir $(0, b)$ a partir de $(b, 0)$. Como sabemos traçar paralelas (ou perpendiculares) segue imediatamente a construção de $(a, b)$ a partir de $(a, 0)$ e $(0, b)$, e isto prova a Proposição 6. ■

Observe que pela Proposição 6 os números construtíveis são exatamente as coordenadas dos pontos construtíveis.

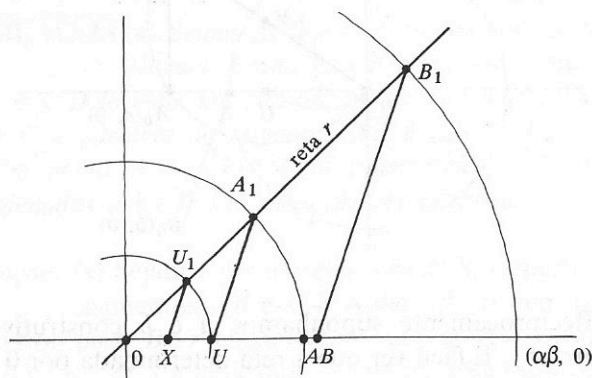
TEOREMA 3. *$\mathscr{C}_{\mathbb{R}} = \{\alpha \in \mathbb{R} : \alpha$ construtível$\}$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$.*

*Demonstração.* Sabemos que $\mathbb{Z} \subset \mathscr{C}_{\mathbb{R}}$. Temos que provar,

(1) $\alpha, \beta \in \mathscr{C}_{\mathbb{R}} \Rightarrow \beta - \alpha \in \mathscr{C}_{\mathbb{R}}$
(2) $\alpha, \beta \in \mathscr{C}_{\mathbb{R}} \Rightarrow \alpha \cdot \beta \in \mathscr{C}_{\mathbb{R}}$
(3) $0 \neq \alpha \in \mathscr{C}_{\mathbb{R}} \Rightarrow \dfrac{1}{\alpha} \in \mathscr{C}_{\mathbb{R}}$.

Vamos assumir, sem perda de generalidade, $\beta > \alpha > 0$. Seja $A = (\alpha, 0)$ e $B = (\beta, 0)$. Pelo item (b) da Proposição 5 segue imediatamente que podemos construir $X$ à direita de 0 sobre a reta $\overline{OU}$ tal que $|\overline{OX}| = |\overline{AB}|$ e isto nos diz que $X = (\beta - \alpha, 0)$ e isto demonstra (1).

Antes de demonstrar a validade de (2) e (3) observe que existem retas construtivas contendo 0 além das retas $\overline{OU}$ e $\overline{OT}$ onde $T = (0, 1)$.

Seja $r$ uma reta construtível como na figura abaixo e sejam $A_1$, $B_1 \in r$ construidos de modo que $|\overline{OA_1}| = |\overline{OA}| = \alpha$, e reta $\overline{BB_1}$ seja paralela a reta $\overline{UA_1}$. Por semelhança de triângulos temos que $\dfrac{\alpha}{1} = \dfrac{|\overline{OB_1}|}{\beta}$ e isto nos diz que $|\overline{OB_1}| = \alpha \cdot \beta$ e daí segue imediatamente que $\alpha \cdot \beta$ é construtível.

Na figura acima seja $U_1 \in r$ tal que $|\overline{OU_1}| = 1$ e $X \in \overline{OU}$ tal que $\overline{XU_1}$ seja paralela a $\overline{UA_1}$. Segue imediatamente da semelhança de triângulos que $|\overline{OX}| = \dfrac{1}{\alpha}$ e portanto $\dfrac{1}{\alpha}$ é construtível. E isto demonstra o Teorema 5. ∎

Antes de demonstrar o próximo teorema vamos dar algumas definições.

Se $A = (u, v) \in \mathscr{P}_n$ dizemos que $u$ e $v$ *são coordenadas de* $\mathscr{P}_n$, e denotaremos por $\mathscr{A}_n$ o conjunto de todas as coordenadas de $\mathscr{P}_n$. Sabemos pela Proposição 8 que $\mathscr{A}_n \subset \mathscr{C}_{\mathbb{R}}\ \forall\, n \in \mathbb{N}$.

Seja $K_0 = \mathbb{Q}, K_1 = \mathbb{Q}[\mathscr{A}_1], \ldots, K_n = \mathbb{Q}[\mathscr{A}_n], \ldots$

Como $\mathscr{A}_0 \subset \mathscr{A}_1 \subset \ldots \subset \mathscr{A}_n \subset \ldots \subset \mathscr{C}_{\mathbb{R}}$ e $\mathbb{Q} \subset \mathscr{C}_{\mathbb{R}}$, temos:

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n \subset K_{n+1} \subset \ldots \subset \mathscr{C}_{\mathbb{R}}.$$

Observe também que se $\alpha \in \mathscr{C}_{\mathbb{R}}$ então $(\alpha, 0) \in \mathscr{P}_n$ para algum $n$, isto é, $\alpha \in \mathscr{A}_n$ para algum $n$, e portanto $\alpha \in K_n$. Daí segue imediatamente que:

$$K_\infty = \bigcup_{n=0}^{\infty} K_n = \mathscr{C}_{\mathbb{R}}.$$

Nós vamos usar essa interpretação de $\mathscr{C}_{\mathbb{R}}$ para provarmos o teorema crucial desse parágrafo.

TEOREMA 4. *$\mathscr{C}_{\mathbb{R}}$ é uma extensão algébrica dos racionais tal que $\forall\, \alpha \in \mathscr{C}_{\mathbb{R}}$ temos que o grau $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ é uma potência de 2.*

*Demonstração.* É bastante provarmos que $\forall\, \alpha \in \mathscr{C}_{\mathbb{R}}$ tem-se que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 2^r$ para algum $r \in \mathbb{N}$.

De fato, seja $\alpha \in \mathscr{C}_{\mathbb{R}} = \bigcup_{n=0}^{\infty} K_n$. Assim $\exists\, n \in \mathbb{N}$ tal que $\alpha \in K_n = \mathbb{Q}[\mathscr{A}_n]$. Como $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ divide $[K_n : \mathbb{Q}]$ (pela Proposição 4) é suficiente provarmos que $[K_n : \mathbb{Q}] = 2^s$ para algum $s \in \mathbb{N}$.

Vamos provar que $[K_n : \mathbb{Q}]$ é potência de 2 por indução sobre $n$. Se $n = 0$ temos $K_0 = \mathbb{Q}$ e o teorema é válido. [se $n = 1$ temos que $K_1 = \mathbb{Q}[\sqrt{3}]$ e o teorema também é válido].

Vamos supor por indução que $[K_i : \mathbb{Q}]$ é potência de 2 $\forall\, 0 \leq i < n$, e vamos provar que $[K_n : \mathbb{Q}]$ é potência de 2.

Como $K_{n-1} \subset K_n$ e $[K_n : \mathbb{Q}] = [K_n : K_{n-1}] \cdot [K_{n-1} : \mathbb{Q}]$ temos que é suficiente provarmos que $[K_n : K_{n-1}]$ é potência de 2.

Seja $L = K_n$ e $L_0 = K_{n-1}$. Sabemos que $L = L_0[\mathscr{A}_n]$. Se $\mathscr{A}_n = \{a_1, \ldots, \alpha_k\}$ temos então que $L = L_0[\alpha_1, \alpha_2, \ldots, \alpha_k]$.

Se denotarmos, $L_0 \subset L_1 = L_0[\alpha_1] \subset L_2 = L_1[\alpha_2] \subset \ldots \subset L_i = L_{i-1}[\alpha_i] \subset \ldots \subset L_k = L$ então é suficiente provarmos que $[L_i : L_{i-1}]$ é potência de 2.

De fato, vamos provar que $[L_i : L_{i-1}] = 1$ ou $2, 1 \leq i \leq k, L_i = L_{i-1}[\alpha_i]$ e $\alpha_i \in \mathscr{A}_n$. Assim $\exists\, \beta_i \in \mathscr{A}_n$ tal que $A_i = (\alpha_i, \beta_i)$ ou $B_i = (\beta_i, \alpha_i) \in \mathscr{P}_n$. Sem perda de generalidade vamos supor que $A_i = (\alpha_i, \beta_i) \in \mathscr{P}_n$.

Como $\mathscr{P}_n = \langle \mathscr{P}_{n-1} \rangle$ temos que $A_i = (\alpha_i, \beta_i)$ é obtido por uma das 3 operações elementares em $\mathscr{P}_{n-1}$. Pode-se provar sem grandes dificuldades que $\alpha_i$ terá que satisfazer uma equação de grau menor ou igual a 2 (será grau 1 na operação elementar I) com coeficientes sobre o corpo $K_{n-1} = \mathbb{Q}[\mathscr{A}_{n-1}]$.

Ora, como $K_{n-1} = L_0 \subset L_{i-1}$ $1 \leq i \leq k$ segue que $\alpha_i$ é raiz de um polinômio de grau 1 ou 2 sobre o corpo $L_{i-1}$ e isto nos diz que $[L_i : L_{i-1}] = 1$ ou 2 como queríamos demonstrar. ■

PROPOSIÇÃO 7. (a) Se $n$ é um número ímpar $\geq 3$ e $p$ um número primo $\geq 2$ então $\sqrt[n]{p}$ não é construtível. Em particular $\sqrt[3]{2}$ não é construtível.

(b) $u = \cos \dfrac{2\pi}{18}$ não é construtível.

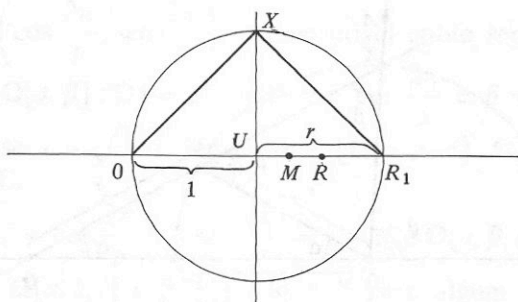
(c) Se $r \geq 0$ é um número construtível então $\sqrt{r}$ também é construtível. Em particular $\sqrt[2^i]{m}$ é construtível $\forall\, i, m \in \mathbb{N}$.

*Demonstração.* (a) Se $\alpha = \sqrt[n]{p}$ $n$ ímpar $\geq 3$, $p$ primo $\geq 2$, então $\operatorname{irr}(\alpha, \mathbb{Q}) = x^n - p$ e portanto $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ ímpar e assim $\alpha$ não é construtível.

(b) Se $\theta = \dfrac{2\pi}{18}$ então $3\theta = \dfrac{2\pi}{6}$. Sabemos que, $\dfrac{1}{2} = \cos 3\theta = 4 \cos^3\theta - 3 \cos\theta$ e daí segue, $8 \cos^3\theta - 6 \cos\theta - 1 = 0$, isto é, $u = \cos\dfrac{\pi}{18}$ é raiz do polinômio $p(x) = 8x^3 - 6x - 1$. Como $p(x)$ é irredutível sobre $\mathbb{Q}$, temos $[\mathbb{Q}[u] : \mathbb{Q}] = 3$ e portanto $u$ não é construtível.

(c) Seja $R = (r, 0)$ e seja $R_1 = (1 + r, 0)$. Assim, como $r$ é construtível segue que $R$ e $R_1$ são construtíveis. Seja $s$ a reta (construtível) perpendicular a $\overline{OU}$ passando por $U$ e seja $M$ o ponto médio do segmento $\overline{OR_1}$.

Pela geometria elementar o ponto $X \in \mathscr{P}_\infty$, como na figura seguinte, é tal que $|\overline{UX}| = \sqrt{r}$.

Assim segue imediatamente pelo item (b) da Proposição 8 que $\sqrt{r}$ é construtível, como queríamos demonstrar.

Os problemas clássicos da duplicação do cubo, da quadratura do círculo e da trissecção do ângulo, que por muito tempo foram preocupações dos gregos serão respondidos no seguinte teorema.

TEOREMA 5. (a) $\nexists\, \alpha \in \mathscr{C}_{\mathbb{R}}$, *tal que o volume do cubo de aresta* $\alpha$ *seja o dobro do volume do cubo de aresta* 1.

(b) $\nexists\, \alpha \in \mathscr{C}_{\mathbb{R}}$, *tal que a área do quadrado de lado* $\alpha$ *seja igual a área do círculo de raio* 1.

(c) *É impossível, com o uso apenas de régua (sem marcas) e compasso, trissectar o ângulo de* 60°.

*Demonstração.* (a) Claramente $\alpha^3 = 2$, ou seja $\operatorname{irr}(\alpha, \mathbb{Q}) = x^3 - 2$ e $[\mathbb{Q}[\alpha]:\mathbb{Q}] = 3$ e pelo teorema anterior segue que $\alpha$ não é construtível.

(b) Como $\alpha^2 = \pi$ e $\pi$ é transcendente sobre $\mathbb{Q}$, segue que $\pi \notin \mathscr{C}_{\mathbb{R}}$ e portanto $\alpha \notin \mathscr{C}_{\mathbb{R}}$.

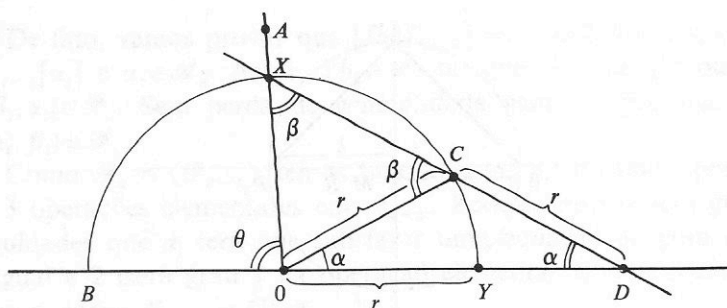
(c) Se $\theta = \dfrac{2\pi}{18} \in \mathscr{C}_{\mathbb{R}}$ podemos ver facilmente que $u = \cos\theta$ também seria construtível, mas isto contraria o item (b) da proposição anterior. ■

EXEMPLO 1. Vamos ver agora, como exemplo, a construção da trissecção de um ângulo $\theta$ usando régua (com marcas, indicando segmentos de comprimento igual a $r$) e compasso.

Na figura seguinte seja $\theta$ o ângulo $AOB$ e consideremos os pontos $X$ e $Y$ como na figura seguinte onde $|\overline{OX}| = |\overline{OY}| = r$.

Provaremos que é possível marcar pontos $C$ e $D$ como na figura seguinte onde $|\overline{CD}| = r$.

De fato, mantendo uma extremidade da régua no ponto $X$ temos que a distância entre pontos alinhados com $X$, um sobre a circun-

ferência e outro sobre a reta $OY$, varia de zero (quando ambas coincidem com $Y$) até $\infty$ (no caso em que a régua passando por $X$ está paralela a $OY$).

Assim, por continuidade $\exists\, D, C$ como na figura tais que $|\overline{CD}| = r$.

Seja $\alpha$ o ângulo $\widehat{CDY}$ da figura acima. Vamos provar que $\alpha = \dfrac{\theta}{3}$. Basta observar na figura que, $\theta = \alpha + \beta$ e $\beta = 2\alpha$, ou seja, $\theta = 3\alpha$ como queríamos demonstrar.

Para encerrar o capítulo falaremos brevemente sobre polígonos regulares.

Um polígono diz-se *construtível* se todos os seus vértices são pontos construtíveis de $\mathbb{R}^2$.

Assim segue imediatamente que, um polígono regular de $n$ lados é construtível se e somente se o ponto $A_n = \left(\cos\dfrac{2\pi}{n}, \operatorname{sen}\dfrac{2\pi}{n}\right)$ é um ponto construtível de $\mathbb{R}^2$.

**PROPOSIÇÃO 8.** (a) *Todo polígono regular de $n = 2^r$ lados é construtível.*

(b) *Se um polígono regular de n lados é construtível então o polígono regular de 2n lados também é construtível.*

(c) *Se p é um número primo $\geq 3$ e um polígono regular de p lados é construtível então $\exists\, s \in \mathbb{N}$ tal que $p = 2^{2^{s}} + 1$. Em particular o heptágono regular não é um polígono construtível.*

*Demonstração.* Os itens (a) e (b) seguem diretamente dos seguintes fatos:

(i) o quadrado é um polígono construtível.

(ii) É possível bissectar um ângulo com régua e compasso.

Agora vamos provar o item (c).

Como $\left(\cos\dfrac{2\pi}{p}, \operatorname{sen}\dfrac{2\pi}{p}\right)$ é construtível então segue pelo Teorema 6 que $[\mathbb{Q}[\alpha,\beta]:\mathbb{Q}] = 2^m$ onde $\alpha = \cos\dfrac{2\pi}{p}$ e $\beta = \operatorname{sen}\dfrac{2\pi}{p}$.

Agora se $i = \sqrt{-1}$ temos que $[\mathbb{Q}[\alpha,\beta,\ i]:\mathbb{Q}] = 2^{m+1}$ onde $\mathbb{Q}[\alpha,\beta,i] \subset \mathbb{C}$.

Agora $\zeta = \cos\dfrac{2\pi}{p} + i\,sen\,\dfrac{2\pi}{p} = \alpha + i\beta \in \mathbb{Q}[\alpha,\beta,i]$ e daí segue que $\mathbb{Q}[\zeta] \subset \mathbb{Q}[\alpha,\beta,i]$ e $[\mathbb{Q}[\zeta]:\mathbb{Q}] = 2^r$ para algum $r \in \mathbb{N}$.

Ora sabemos que $\operatorname{irr}(\zeta,\mathbb{Q}] = x^{p-1} + x^{p-2} + \ldots + x + 1$ e portanto segue que $p - 1 = 2^r$, isto é, $p = 2^r + 1$.

Vamos provar que $r = 2^s$ para algum $s \in \mathbb{N}$. De fato, se $t$ é um fator ímpar de $r$ com $t > 1$ temos $r = t \cdot v$.

Daí segue,

$$p = 2^r + 1 = (2^v)^t + 1 \text{ onde } t \text{ é ímpar} > 1$$

e temos,

$$p = (2^v + 1)((2^v)^{t-1} - (2^v)^{t-2} + (2^v)^{t-3} - \ldots \pm 1)$$

contradizendo o fato de $p$ ser primo, e isto demonstra a Proposição 8. ■

Enunciaremos agora sem demonstração o seguinte teorema:

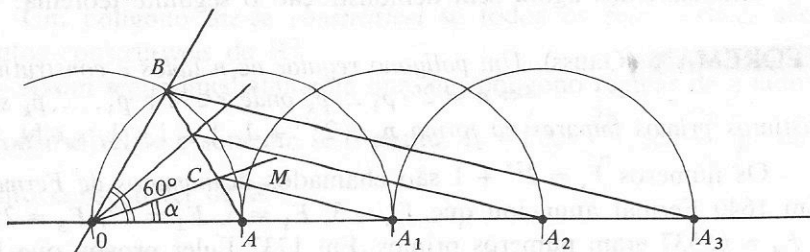
TEOREMA 6 (Gauss). *Um polígono regular de n lados é construtível* $\Leftrightarrow n = 2^r \cdot p_1 \ldots p_k$ *onde* $r \in \mathbb{N}$ *e* $p_1, \ldots, p_k$ *são distintos primos impares na forma* $p_i = 2^{2^{s_i}} + 1$, $1 \le i \le k$, $s_i \in \mathbb{N}$.

Os números $F_s = 2^{2^s} + 1$ são chamados de *números de Fermat*. Em 1640 Fermat anunciou que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$ eram números primos. Em 1732 Euler provou que $F_5$ é divisível por $5 \cdot 2^7 + 1$. Os únicos números primos de Fermat conhecidos são aqueles anunciados pelo próprio Pierre de Fermat.

## EXERCÍCIOS

$O$ e $U$ serão considerados sempre $O = (0,0)$ e $U = (1,0)$.

1. Prove que $\langle \mathscr{P}_\infty \rangle = \mathscr{P}_\infty$ e que $(m,0) \in \mathscr{P}_\infty\ \forall\, m \in \mathbb{Z}$.
2. Seja $\mathscr{A}_n$ o conjunto de coordenadas de $\mathscr{P}_n$ e $K_n = \mathbb{Q}[\mathscr{A}_n]$. Prove que $K_1 = \mathbb{Q}[\sqrt{3}]$, e mais $K_\infty = \bigcup_{n=0}^{\infty} K_n = \mathscr{C}_{\mathbb{R}}$.
3. Se $A, B \in \mathscr{P}_\infty$ prove que $\exists\, A_1, B_1 \in \mathscr{P}_\infty$ tais que: $A_1$, $B_1$ estão sobre a reta $\overline{OU}$ e $|\overline{AB}| = |\overline{A_1 B_1}|$.

4. Prove que um quadrilátero $ABCD$ em $\mathbb{R}^2$ que possui lados opostos iguais é um paralelogramo.
5. Seja $(\alpha, \beta) \in \mathscr{P}_n = \langle \mathscr{P}_{n-1} \rangle$ e $K_{n-1} = \mathbb{Q}[\mathscr{A}_{n-1}]$ como no Exercício 2. Prove que $[K_{n-1}[\alpha] : K_{n-1}] = 1$ ou 2.
6. Prove que um polígono regular de $n$ lados no plano é construtível $\Leftrightarrow$ o ponto $\left(\cos\frac{2\pi}{n}, \operatorname{sen}\frac{2\pi}{n}\right)$ é construtível.
7. Prove que os polígonos regulares de 3 e 5 lados (respectivamente, o triângulo e o pentágono) são construtíveis. Prove também que se $n = 2^r \cdot 3$ ou $2^r \cdot 5$ então o polígono regular de $n$ lados é construtível.
8. Prove que um eneágono regular não é construtível.
9. Prove que um polígono regular de 15 lados é construtível. (*sugestão*: use $\frac{2\pi}{15} = \frac{4\pi}{5} - \frac{2\pi}{3}$, e use o Exercício 7).
10. Mostre que a construção abaixo não trissecta o ângulo de 60°. sejam $AOB = 60°$, $|\overline{AA_1}| = |\overline{A_1A_2}| = |\overline{A_2A_3}|$ e seja $\overline{BA_3}$ paralela a $\overline{CA_1}$. (Prove então que $d = \widehat{AOM} \neq 20°$).

11. Se um polígono regular de $n$ lados é construtível e $m$ é um divisor de $n$, então podemos construir um polígono regular de $m$ lados.
(*Sugestão*: escolha (entre os vértices do polígono de $n$ lados) adequadamente os vértices do polígono de $m$ lados).
12. Prove que se um polígono regular de $m$ lados e um polígono regular de $n$ lados são construtíveis e M.D.C. $\{m, n\} = 1$ então um polígono regular de $m \cdot n$ lados também é construtível.
(*Sugestão*: escreva $\frac{2\pi}{mn} = a \cdot \frac{2\pi}{m} + b \cdot \frac{2\pi}{n}$ onde $a, b \in \mathbb{Z}$ e expresse $\cos\frac{2\pi}{mn}$).

# GRUPOS

Neste capítulo temos como objetivo introduzir os aspectos elementares da teoria dos grupos que serão usados no capítulo seguinte onde demonstraremos o teorema fundamental da Teoria de Galois.

## §1 Definição e exemplos

Seja $G$ um conjunto não vazio onde está definida uma operação entre pares de $G$, denotada por,

$$\begin{aligned} *: G \times G &\to G \\ (x, y) &\rightsquigarrow x * y \end{aligned}$$

Dizemos que o par $G, *$ é um grupo se são válidas as seguintes propriedades:

$G_1$) $a * (b * c) = (a * b) * c \quad \forall\, a, b, c, \in G$
$G_2$) $\exists e \in G$ tal que $a * e = e * a, \quad \forall\, a \in G$
$G_3$) $\forall\, a \in G, \exists b \in G$ tal que $a * b = b * a = e$.

A propriedade $G_1$) é a *associatividade* da operação $*$, enquanto que o elemento e em $G_2$), pode-se provar facilmente que é único, recebe o nome de *identidade* de $G, *$.

Agora se $a * b_1 = b_1 * a = e, \; a * b_2 = b_2 * a = e$ segue que $b_1 = e * b_1 = (b_2 * a) * b_1 = b_2 = b_2 * (a * b_1) = b_2$, e portanto em $G_3$) existe um único elemento $b \in G$ tal que $a * b = b * a = e$. Tal elemento $b$ é denotado por $a^{-1}$ e recebe o nome de *inverso de a* em relação a operação $*$.

Se em um grupo $G, *$ verifica-se a propriedade:

$G_4$) $a * b = b * a, \quad \forall\, a, b \in G$

dizemos que o grupo $G, *$ é um *grupo abeliano* (em honra ao matemático Norueguês N.H. Abel – 1802-1829).

A fim de simplificar notações usaremos $G$ em vez de $G, *$, para denotar um grupo. Usaremos também $ab$, em vez de $a * b$, para representar o resultado de $a$ operado com $b$. A operação de $G$ será sempre

explicitada no contexto, e usaremos a notação aditiva $a * b = a + b$ apenas para grupos abelianos e nesse caso a identidade será representada por $O$.

EXEMPLO 1. $\mathbb{Z}$ é um grupo aditivo infinito.

EXEMPLO 2. Se $n \geq 1$ é um número inteiro então o conjunto $\mathbb{Z}_n$ dos inteiros módulo $n$, é um grupo aditivo contendo exatamente $n$ elementos.

EXEMPLO 3. Seja $S$ um conjunto não vazio e seja

$$G = \{f : S \to S : f \text{ bijetiva}\}.$$

Se $*$ é a operação composição de funções, isto é, $* : G \times G \to G$, $(g, f) \rightsquigarrow g \circ f$

então $G, *$ é claramente um grupo tendo $I_S : S \to S$, $x \rightsquigarrow x$ como identidade.

Esse grupo é chamado de *grupo das Permutações do conjunto S*. Se $S = \{1, 2, \ldots, n\}$ denotaremos esse grupo por $S_n$, e temos que o número de elementos de $S_n$ é exatamente $n!$.

Agora vamos mostrar que os grupos $S_n$, $n \geq 3$, são exemplos de grupos não abelianos.

De fato, sejam $f, g \in S_n$ definidas como segue:

$$f : \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, n\}$$

$$f(1) = 2, \quad f(2) = 1, \quad f(x) = x \quad \forall x, \quad 3 \leq x \leq n$$

$$g : \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, n\}$$

$$g(1) = 2, \quad g(2) = 3, \quad g(3) = 1 \text{ e se } n \geq 4 \quad g(x) = x \quad \forall x, \quad 4 \leq x \leq n$$

Ora, como

$$(g \circ f)(1) = g(f(1)) = g(2) = 3.$$
$$(f \circ g)(1) = f(g(1)) = f(2) = 1.$$

teremos que $g \circ f \neq g \circ g$.

Em particular $S_3$ é um exemplo de um grupo não abeliano com exatamente 6 elementos. No próximo parágrafo provaremos que: "se um grupo $G$ possui no máximo 5 elementos então $G$ é um grupo abeliano".

É usual denotar um elemento $f$ do grupo $S_n$ por,

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}.$$

Assim o grupo $S_3$ é composto dos seguintes 6 elementos:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad ; \; f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_1^{-1}$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_2^{-1}; \; f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_3^{-1}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5^{-1}; \; f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_4^{-1}$$

EXEMPLO 4. Seja $G$ o conjunto de retas no plano $\mathbb{R}^2$ com coeficiente angular não nulo, isto é,

$$G = \{f : \mathbb{R} \to \mathbb{R} : f(x) = ax + b, \; 0 \neq a, b \in \mathbb{R}\}$$

Se $f(x) = ax + b$, $a \neq 0$ e $g(x) = cx + d$, $c \neq 0$ então

$$(g \circ f)(x) = g(f(x)) = acx + (bc + d), \; ac \neq 0$$

ou seja a composição de funções $\circ$ define uma operação em $G$ que é evidentemente associativa.

Agora, $e = I_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$, $x \rightsquigarrow x$ é um elemento de $G$ e mais se $f^{-1}(x) = \frac{1}{a}x - \frac{b}{a}$, $a \neq 0$, temos:

$$f^{-1} \circ f = f \circ f^{-1} = I_{\mathbb{R}} \text{ onde } f(x) = ax + b, \; a \neq 0.$$

Assim, $G, \circ$ é um grupo onde $\circ$ é a operação composição de funções.

Se $f(x) = 2x + 4$ e $g(x) = 3x + 2$ temos,
$(g \circ f)(x) = g(f(x)) = g(2x + 4) = 6x + 14$
$(f \circ g)(x) = f(3x + 2) = 6x + 8$

Portanto $G, \circ$ é um exemplo de um grupo não abeliano contendo um número infinito de elementos.

EXEMPLO 5. Vamos definir agora o seguinte subconjunto $Q_8$ do anel dos Quatérnios visto no Capítulo 3.

Seja $Q_8 = \{1, -1, i, j, k, -i, -j, -k\} \subset \text{Quat}$

É fácil de ver que $Q_8$ é um grupo com a operação de multiplicação de Quat pois,

$$i^2 = j^2 = k^2 = -1, \; x \cdot 1 = 1 \cdot x = x \;\; \forall x \in Q_8$$

e

$$i \cdot j = k, \; j \cdot k = i, \; k \cdot i = j, \; j \cdot i = -k, \; k \cdot j = -i, \; i \cdot k = -j$$

Além disso, $j^{-1} = j^3 = -j$, $k^{-1} = -k$, $i^{-1} = -i$.

Assim $Q_8, \cdot$ é um grupo não abeliano contendo exatamente 8 elementos.

EXEMPLO 6. Seja $A, +, \cdot$ um anel e $G = \text{Aut}\, A$ o conjunto de todos os automorfismos do anel $A$.

Primeiramente observem que se $g, f \in G$ e $a, b \in A$, então $(g \circ f)(a+b) = g[f(a+b)] = g[f(a)+f(b)] = g[f(a)] + g[f(b)] = = (g \circ f)(a) + (g \circ f)(b)$.

Analogamente $(g \circ f)(a \cdot b) = (g \circ f)(a) \cdot (g \circ f)(b)$, ou seja, a composição de funções define uma operação entre pares de elementos de $G = \text{Aut}\, A$.

Observem também que $e = I_A : A \to A$ é um elemento de $G$.
$x \rightsquigarrow x$

Como composição de funções é uma operação associativa para que $G, \circ$ seja um grupo é suficiente mostrarmos que $G$ é fechado para o inverso de cada elemento, isto é, se $f \in G$ então a função $g = f^{-1}$ (existe pois $f$ é bijetiva) é também um automorfismo do anel $A$. De fato, seja $f \in G$ e $g : A \to A$ definida por $f \circ g = g \circ f = I_A$. Vamos provar que $g \in G$.

Se $x', y' \in A$ então temos que provar que:

(i) $g(x' + y') = g(x') + g(y')$
(ii) $g(x' \cdot y') = g(x') \cdot g(y')$.

Agora se $x', y' \in A$ e $f$ bijetiva então $\exists\, x, y \in A$ tais que $x' = f(x)$ e $y' = f(y)$ (e portanto $x = g(x')$ e $y = g(y')$).

Assim,

(i) $g(x' + y') = g(f(x) + f(y)) = g(f(x+y)) = x + y = g(x') + g(y')$

e

(ii) $g(x' \cdot y') = g(f(x) \cdot f(y)) = g(f(x \cdot y)) = x \cdot y = g(x') \cdot g(y')$

e isto prova que $G = \text{Aut } A, \circ$ é um grupo onde $\circ$ é a operação composição de funções.

Observem que já calculamos, no §4 do Capítulo 3, o grupo $G = \text{Aut } A$ para alguns anéis. Por exemplo, $\text{Aut } \mathbb{Z} = \{I_{\mathbb{Z}}\}$, $\text{Aut } \mathbb{Q} = \{I_{\mathbb{Q}}\}$, $\text{Aut } \mathbb{R} = \{I_{\mathbb{R}}\}$ e $\text{Aut } \mathbb{Z}[\sqrt{p}] = \{I_{\mathbb{Z}[\sqrt{p}]}, \sigma\}$ onde $p$ é um número primo e $\sigma.(a + b\sqrt{p}) = a - b\sqrt{p}\ \forall a, b \in \mathbb{Z}$.

EXEMPLO 7. Seja $G$ um grupo e $x \in G$. Se $n \in \mathbb{Z}$ definimos $x^n$ como segue:

$$x^n = \begin{cases} e & \text{se} \quad n = 0 \\ x^{n-1} \cdot x & \text{se} \quad n > 0 \\ (x^{-n})^{-1} & \text{se} \quad n < 0 \end{cases}$$

Se $m, n \in \mathbb{Z}$ pode-se provar, usando indução, as seguintes propriedades:

(i) $x^m \cdot x^n = x^{m+n}$

(ii) $(x^m)^n = x^{mn}$

Se denotarmos $\langle x \rangle = \{x^m : m \in \mathbb{Z}\} \subset G$ então como $x^0 = e$, $(x^m)^{-1} = x^{-m}$ e $x^m \cdot x^n = x^{m+n}$ segue imediatamente que $\langle x \rangle$ é um exemplo de grupo abeliano. O grupo $\langle x \rangle$ é chamado de *Grupo cíclico* gerado pelo elemento $x \in G$. Assim todo grupo cíclico é abeliano. Pode-se verificar facilmente que os grupos aditivos $\mathbb{Z}$ e $\mathbb{Z}_n$, citados nos exemplos 1 e 2, são cíclicos.

Vamos ver em seguida um exemplo de um grupo abeliano não cíclico.

EXEMPLO 8. Sejam $G, \circ$ e $H, \Delta$ dois grupos cujas identidades representaremos respectivamente por $e_G$ e $e_H$.

Seja $G \times H = \{(g, h) : g \in G \text{ e } h \in H\}$ o conjunto produto cartesiano de $G$ e $H$. Vamos definir uma operação $*$ entre pares de elementos de $G \times H$ através da regra,

$$(g, h) * (g', h') = (g \circ g', h \Delta h') \quad \forall\, g, g' \in G, \quad \forall\, h, h' \in H.$$

É fácil verificar que $e = (e_G, e_H)$ é tal que, $(g, h) * e = e * (g, h) = (g, h)\ \forall (g, h) \in G \times H$ e $e = (g, h) * (g^{-1}, h^{-1}) = (g^{-1}, h^{-1}) * (g, h)\ \forall (g, h) \in G \times H$.

Assim, como a transitividade da operação $*$ decorre imediatamente da transitividade das operações $\circ$ e $\Delta$ temos que $G \times H, *$ é um grupo com identidade $e = (e_G, e_H)$.

Observem que se $G, \circ$ e $H, \Delta$ são grupos abelianos então $G \times H, *$ também é um grupo abeliano.

Se $G, \circ$ e $H, \Delta$ são grupos aditivos usaremos também a notação aditiva para $G \times H, *$.

Assim se $G, +$ e $H, +$ são grupos, então $G \times H, +$ é também um grupo onde,

$$(g, h) + (g', h') = (g+g', h+h'), \quad \forall\, g, g' \in G, \quad \forall\, h, h' \in H.$$

Sabemos que $\mathbb{Z}_4, +$ é um exemplo de um grupo cíclico contendo exatamente 4 elementos. Vamos agora dar um exemplo de um grupo abeliano não cíclico contendo também 4 elementos.

Se $G = \mathbb{Z}_2 \times \mathbb{Z}_2, +$. Assim os elementos de $G$ são $(\overline{0}, \overline{0})$, $(\overline{0}, \overline{1})$, $(\overline{1}, \overline{0})$ e $(\overline{1}, \overline{1})$. Observe que $e = (\overline{0}, \overline{0})$ é a identidade desse grupo $G$ e pode-se verificar facilmente que: $\forall\, (\overline{a}, \overline{b}) \in G$ tem-se:

$$(\overline{a}, \overline{b})^2 = (\overline{a}, \overline{b}) + (\overline{a}, \overline{b}) = (\overline{0}, \overline{0}) = e.$$

Portanto $G = \mathbb{Z}_2 \times \mathbb{Z}_2, +$ é um grupo abeliano não cíclico.

Do mesmo modo que introduzimos o grupo $G \times H$ poderiamos introduzir o grupo $G_1 \times G_2 \times \ldots \times G_n$ que é chamado de produto direto (externo) dos grupos $G_1, \ldots, G_n$.

## EXERCÍCIOS

1. Seja $G$ um grupo e $x \in G$. Prove que
   a) $x^m \cdot x^n = x^{m+n} \quad \forall\, m, n \in \mathbb{Z}$
   b) $(x^m)^n = x^{mn} \quad \forall\, m, n \in \mathbb{Z}$

2. Seja $G$ um grupo. $G$ diz-se *cíclico* se $\exists\, x \in G$ tal que $G = \langle x \rangle$, e o elemento $x$ chama-se um gerador de $G$.
   Prove que:
   a) Todo grupo cíclico é abeliano.
   b) $\mathbb{Z}, +$ é um grupo cíclico tendo $1$ e $-1$ como geradores.
   c) $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}, +$ com $p$ primo é um grupo cíclico tendo $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ como geradores.

3. Seja $G$ é um grupo abeliano. Prove que: Se $x, y \in G$ e $m \in \mathbb{Z}$ então $(xy)^m = x^m \cdot y^m$.

4. Seja $G$ um grupo tendo e como elemento identidade. Prove que: Se $x^2 = e \quad \forall\, x \in G$ então $G$ é um grupo abeliano.

5. Seja $G$ um grupo. Prove a unicidade do elemento neutro de $G$.

6. Determine $f, g \in S_3$ tais que:
   a) $(f \circ g)^3 \neq f^3 \circ g^3$
   b) $(f \circ g)^2 \neq f^2 \circ g^2$
7. a) Determine todos os elementos $f \in S_3$ tais que
$$f^2 = e, \quad f \neq e.$$
   b) Determine todos os elementos $f \in S_3$ tais que
$$f^3 = e, \quad f \neq e.$$
8. Seja $V = \{e, f, g, h\}$ o seguinte subconjunto do grupo $S_4$:
$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}; \quad f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$
$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}; \quad h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$
   a) Prove que $V, \circ$ é um grupo contendo 4 elementos onde $\circ$ é a operação de $S_4$.
   b) Prove que $V, \circ$ é um grupo abeliano não cíclico.
9. Seja $G$ um grupo e $x, y, z \in G$. Prove que:
$$\left.\begin{array}{l} \text{a) } xy = xz \Rightarrow y = z \\ \text{b) } yx = zx \Rightarrow y = z \end{array}\right\} \text{ (leis do cancelamento)}$$
   c) $(xy)^{-1} = y^{-1} \cdot x^{-1}$
   d) $(x^{-1})^{-1} = x$
10. Seja $G$ um grupo contendo exatamente $2n$ elementos, $n \geq 1$ inteiro. Prove que, $\exists\, x \neq e$ tal que $x^2 = e$ onde $e$ representa a identidade de $G$.
11. Seja $G$ um conjunto não vazio finito e $*$ uma operação associativa em $G$.
    Prove que:
    Se são válidas em $G$, $*$ as leis do cancelamento então $G, *$ é um grupo.
12. Seja $G_p = \left\{ \dfrac{m}{p^\alpha} : \begin{array}{l} m \in \mathbb{Z}, \text{ M.D.C. } \{p^\alpha, m\} = 1 \\ \alpha \in \mathbb{N} \end{array} \right\}$ onde $p$ é um número primo fixo. É $G_p, +$ um grupo? Se $\dfrac{1}{p} \in G, +$ calcule o grupo $\left\langle \dfrac{1}{p} \right\rangle$.
    Calcule também $\left\langle \dfrac{1}{p^2} \right\rangle, \left\langle \dfrac{1}{p^3} \right\rangle, \ldots, \left\langle \dfrac{1}{p^n} \right\rangle$ onde $n \in \mathbb{N}$.

13. Calcule Aut $A$ para os seguintes anéis:
a) $A = \mathbb{Z}[i]$ onde $i^2 = -1$
b) $A = \mathbb{Q}[i]$
c) $A = \mathbb{Q}[\sqrt[3]{2}]$ onde $\sqrt[3]{2} = \alpha \in \mathbb{R}$, $\alpha^3 = 2$.

14. Quais dos seguintes subconjuntos $G$ de $\mathbb{Z}_{13} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{12}\}$ são grupos com a operação de multiplicação?
a) $G = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}\}$
b) $G = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}\}$
c) $G = \{\overline{1}, \overline{3}, \overline{5}, \overline{8}, \overline{9}\}$

15. Seja $G, *$ um grupo e $a, b, c \in G$. Prove que a equação $x * a * x * b = x * c$ possui uma única solução em $G$.

16. Prove que $G = \{z \in \mathbb{C} : |z| = 1\}$ é um grupo abeliano com a operação de multiplicação de números complexos.

## §2 Subgrupos e classes laterais

Sejam $G$ um grupo e $H$ um subconjunto não vazio de $G$. Dizemos que $H$ é um *subgrupo de* $G$ se $H$ for ele próprio um grupo com a mesma operação de $G$. Assim para que $H$ seja um subgrupo de $G$ são necessárias as condições (i) $e \in H$ e (ii) se $a, b \in H$ então $ab \in H$. Em geral essas duas condições não são suficientes para que $H$ seja um subgrupo de $G$ ($H = \mathbb{N} \subset \mathbb{Z} = G$ satisfaz as duas condições acima onde a operação é soma, porém não é um subgrupo de $\mathbb{Z}, +$). Provaremos agora uma proposição que fornece as condições necessárias e suficientes para que um subconjunto $H$ de um grupo $G$ seja um subgrupo de $G$. Se $H$ for um subgrupo de $G$ denotaremos $H \leq G$.

**PROPOSIÇÃO 1.** *Seja $G$ um grupo e $H$ um subconjunto de $G$. As seguintes condições são equivalentes:*

(a) *$H$ é um subgrupo de $G$.*
(b) (i) $e \in H$
(ii) $\forall\, a, b \in H$ *tem-se* $ab \in H$
(iii) $\forall\, a \in H$ *tem-se* $a^{-1} \in H$.
(c) $H \neq \emptyset$ e $\forall\, a, b \in H$ *tem-se* $ab^{-1} \in H$.

*Demonstração.* (a) $\Rightarrow$ (b): Segue imediatamente das definições e da unicidade da identidade e da unicidade do inverso de cada elemento de $G$.

(b) ⇒ (a): Basta observar que a condição (ii) ($H$ é fechado para a operação de $G$) nos diz que a operação de $G$ induz uma operação em $H$ e essa operação será também associativa pois a operação é associativa em $G$.

(b) ⇒ (c): Primeiramente, se $e \in H$ então $H \neq \varnothing$, e se $b \in H$ então $b^{-1} \in H$ por (iii).

Assim, se $a, b \in H$ temos $a, b^{-1} \in H$ e por (ii) segue $ab^{-1} \in H$ como queríamos demonstrar.

(c) ⇒ (b): Se $H \neq \varnothing$ então $\exists\, a \in H$. Portanto, $e = aa^{-1} \in H$. Agora, se $a \in H$ segue $a^{-1} = ea^{-1} \in H$, e finalmente se $a, b \in H$ tem-se $a, b^{-1} \in H$ e daí teremos $ab = a(b^{-1})^{-1} \in H$ e isto termina a demonstração da Proposição 1. ■

EXEMPLO 1. $H = \mathbb{Z} \cdot m = \{rm : r \in \mathbb{Z}\}$, $m \in \mathbb{Z}$, é um subgrupo do grupo aditivo dos inteiros.

EXEMPLO 2. Seja $G$ um grupo e $x \in G$. Então $\langle x \rangle = H$ é um subgrupo de $G$.

EXEMPLO 3. Seja $G$ um grupo e $x \in G$. Então, $C_G(x) = \{y \in G : yx = xy\}$ é um subgrupo de $G$. ($C_G(x)$ é denominado o *centralizador de x em G*).

EXEMPLO 4. Seja $G$ um grupo. Então,

$$Z(G) = \{a \in G : a \cdot x = x \cdot a \quad \forall\, x \in G\}$$

é um subgrupo $G$. ($Z(G)$ é denominado de *centro do grupo G*). Observe que $Z(G)$ é um subgrupo abeliano do grupo $G$.

EXEMPLO 5. Sejam $H_1, \ldots, H_n$ subgrupos de um grupo $G$. Então,

$$H = H_1 \cap \ldots \cap H_n$$

é um subgrupo de $G$.

De fato,

(i) $e \in H \neq \varnothing$ pois $e \in H_i \quad \forall\, i \in \{1, \ldots, n\}$

(ii) $a, b \in H \Rightarrow a, b^{-1} \in H_i \quad \forall\, i \in \{1, 2, \ldots, n\} \Rightarrow ab^{-1} \in H$.

EXEMPLO 6. Seja $G$ um grupo e $x_1, x_2, \ldots, x_n \in G$. Seja $\mathscr{F}$ a família de todos os subgrupos de $G$ contendo $x_1, \ldots, x_n$, isto é,

$$\mathscr{F} = \{K \leq G : x_1, \ldots, x_n \in K\}.$$

Ora $G \in \mathscr{F}$, assim $\mathscr{F} \neq \emptyset$. Agora vamos definir $H$ do seguinte modo: $H = \bigcap_{K \in \mathscr{F}} K$, e provaremos em seguida que $H$ é o menor subgrupo de $G$ que contém $x_1, \ldots, x_n$.

Primeiramente $H$ é um subgrupo de $G$.

De fato,

(i) $e \in H \neq \emptyset$ pois $e \in K \quad \forall K \in \mathscr{F}$.
(ii) $a, b \in H \Rightarrow a, b \in K \; \forall K \in \mathscr{F} \Rightarrow a, b^{-1} \in K, \; \forall K \in \mathscr{F} \Rightarrow ab^{-1} \in K$, $\forall K \in \mathscr{F} \Rightarrow ab^{-1} \in H$, e assim $H \leq G$.

Agora provaremos que $H$ é o menor subgrupo de $G$ contendo $x_1, \ldots, x_n$.

De fato,

Seja $L \leq G$ tal que $x_1, \ldots, x_n \in L$. Assim, $L \in \mathscr{F}$ e portanto $H \leq L$.

Denotaremos $H$ por $H = \langle x_1, \ldots, x_n \rangle$. Observe que se $n = 1$ então essa definição coincide com a de grupo cíclico gerado por $x_1$.

EXEMPLO 7. Sejam $H_1 \subseteq H_2 \subseteq \ldots \subseteq H_n \subseteq H_{n+1} \subseteq \ldots$ subgrupos de um grupo $G$. Então,

$$H = \bigcup_{i=1}^{\infty} H_i$$

é um subgrupo de $G$.

De fato,

(i) $e \in H \neq \emptyset$ pois $e \in H_1 \subset H$.
(ii) $a, b \in H \Rightarrow a \in H_r, \; a \in H_s$, onde $r, s \in \{1, 2, \ldots, n, \ldots\}$.

Sem perda de generalidade podemos assumir que $r \leq s$ e nesse caso teremos,

$$a, b \in H_s \text{ pois } H_r \subseteq H_s.$$

Daí segue que $ab^{-1} \in H_s \subset H$.

EXEMPLO 8. Seja $G$ o grupo aditivo dos racionais e

$$H = \left\{ \frac{m}{p^\alpha} : \begin{matrix} m \in \mathbb{Z}, \text{ M.D.C. } \{p^\alpha, m\} = 1 \\ \alpha \in \mathbb{N} \end{matrix} \right\}$$

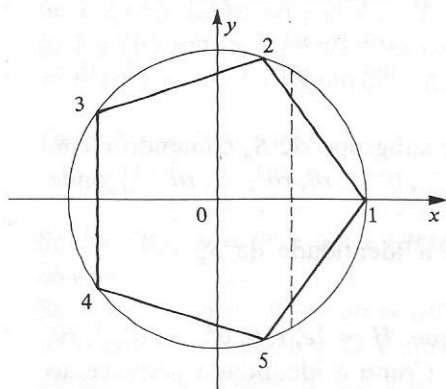
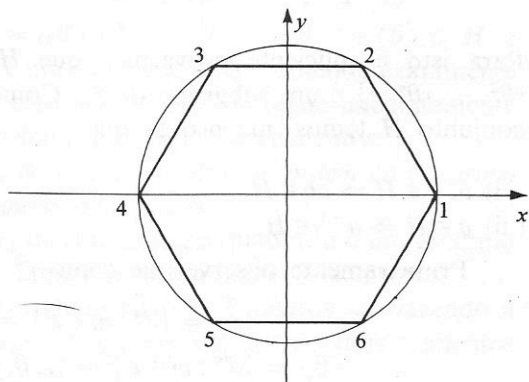
onde $p$ é um número primo fixo. Vimos no parágrafo anterior que $H \leq G$. Agora vamos definir os seguintes subgrupos de $H$:

$$C_p = \left\langle \frac{1}{p} \right\rangle, \quad C_{p^2} = \left\langle \frac{1}{p^2} \right\rangle, \ldots, C_{p^n} = \left\langle \frac{1}{p^n} \right\rangle$$

Observe que $C_p \subset C_{p^2} \subset \ldots \subset C_{p^n} \subset \ldots \subset H$ e é fácil verificar que

$$H = \bigcup_{i=1}^{\infty} C_{p^i}.$$

EXEMPLO 9. Seja $G$ o conjunto de todas as retas do plano $\mathbb{R}^2$ com coeficiente angular não nulo. Sabemos que, $G = \{f : \mathbb{R} \to \mathbb{R} : f(x) = ax + b, 0 \neq a, b \in \mathbb{R}\}$ é um grupo com a operação composição de funções. Se $H$ é o conjunto das retas do plano $\mathbb{R}^2$ com coeficientes angular 1 então é fácil verificar que $H$ é um subgrupo de $G$.

EXEMPLO 10. Seja $\{1, 2, 3, \ldots, n\}$, $n \geq 3$, o conjunto de vértices de um polígono regular de $n$ lados como nas figuras abaixo:

Considerando $S_n$ o grupo (veja Exemplo 3 do §1) de todas as permutações do conjunto de vértices $\{1, 2, 3, ..., n\}$ vamos agora ver um exemplo de um subgrupo de $S_n$, não abeliano, contendo exatamente $2n$ elementos.

Seja $\theta \in S_n$ a permutação determinada pelo efeito de uma rotação de um ângulo de $\frac{2\pi}{n}$ $rd$ no sentido trigonométrico, isto é,

$$\theta = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix}$$

Consideremos $r \in S_n$ a permutação determinada pelo efeito de uma reflexão da figura em torno do eixo $\overline{ox}$, isto é, se $n$ é par $r$ fixa os vértices 1 e $\frac{n+2}{2}$ e é representada por

$$r = \begin{pmatrix} 1 & 2 & 3 & \dots & \frac{n+2}{2} & \dots & n-1 & n \\ 1 & n & n-1 & \dots & \frac{n+2}{2} & \dots & 3 & 2 \end{pmatrix}$$

se $n$ é ímpar $r$ fixa apenas o vértice 1 e é representada por

$$r = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}.$$

Agora, seja $D_n = \langle r, \theta \rangle$ o menor subgrupo de $S_n$ contendo $r$ e $\theta$. Vamos provar que $D_n = \{e, r, \theta, \theta^2, ..., \theta^{n-1}, r\theta, r\theta^2, ..., r\theta^{n-1}\}$ onde $e = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & 2 & 3 & \dots & n-1 & n \end{pmatrix}$ é a identidade de $S_n$.

Para isto é suficiente provarmos que $H = \{e, r, \theta, \theta^2, ..., \theta^{n-1}, r\theta, r\theta^2, ..., r\theta^{n-1}\}$ é um subgrupo de $S_n$. Como a identidade pertence ao conjunto $H$ temos que provar que:

(i) $a, b \in H \Rightarrow ab \in H$.
(ii) $a \in H \Rightarrow a^{-1} \in H$.

Primeiramente observe que como $r^2 = e$ e $\theta^n = e$ então temos,

$$\langle r \rangle = \{r^m : m \in \mathbb{Z}\} = \{e, r\}$$
$$\langle \theta \rangle = \{\theta^m : m \in \mathbb{Z}\} = \{e, \theta, \theta^2, ..., \theta^{n-1}\}$$

É também imediata a verificação das seguintes leis:

(1) $r \cdot \theta^i = \theta^{-i} \cdot r \quad \forall\, i \in \mathbb{N}$
(2) $\theta^j \cdot r = r \cdot \theta^{-j} \quad \forall\, j \in \mathbb{N}$

ou equivalentemente,

(3) $r \cdot \theta^m = \theta^{-m} \cdot r \quad \forall\, m \in \mathbb{Z}$

Usando esta lei provaremos inicialmente

(iii) $a \in H \Rightarrow a^{-1} \in H$.

se $a = \theta^k$, $0 \leq k \leq n-1$ então $a^{-1} = \theta^{n-k} \in H$
se $a = r \cdot \theta^k$, $0 \leq k \leq n-1$ então teremos,

$$a^2 = (r\theta^k)(r\theta^k) = r(\theta^k r)\theta^k = r^2\theta^{-k}\theta^k = r^2 = e.$$

Assim $a = a^{-1} \in H$ e (iii) está provada.
Agora vamos provar (ii) $a, b \in H \rightarrow ab \in H$.
Observe que $\theta^m \in \langle\theta\rangle = \{e, \theta, \ldots, \theta^{n-1}\}$ $\forall m \in \mathbb{Z}$.

*Caso* 1: $a \in \langle\theta\rangle$, $b \in H$.

$$a = \theta^j, \quad 0 \leq j \leq n-1.$$

Se $b \in \langle\theta\rangle$ então $ab \in \langle\theta\rangle \subseteq H$
se $b \notin \langle\theta\rangle$ então $b = r\theta^i$, $0 \leq i \leq n-1$ e nesse caso teríamos $ab =$ $= \theta^j(r\theta^i) = r\theta^{i-j}$ e como $\theta^{i-j} \in \langle\theta\rangle$ segue $ab \in H$.

*Caso* 2: $a \notin \langle\theta\rangle$, $b \in H$.

$$a = r\theta^i$$

Se $b \in \langle\theta\rangle$, $b = \theta^j$ e $ab = (r\theta^i)\theta^j = r\theta^{i+j}$ e como $\theta^{i+j} \in \langle\theta\rangle$ segue $ab \in H$.
Se $b \notin \langle\theta\rangle$, $b = r\theta^j$ e $ab = (r\theta^i)(r\theta^j) = r^2\theta^{j-i} = \theta^{j-i} \in \langle\theta\rangle \subseteq H$ e isto demonstra que $H = D_n$ é um subgrupo de $S_n$ contendo exatamente $2n$ elementos. Como $n \geq 3$ e $r\theta = \theta^{-1} \cdot r \neq \theta r$ segue imediatamente que $D_n$ é um grupo não abeliano contendo $2n$ elementos.

Chamamos o grupo $D_n$ de *grupo ihedral de ordem* $2n$ ou *grupo de simetrias do polígono regular de n lados*.

Observe que o grupo $D_4$ de simetrias do quadrado é um exemplo de um grupo não abeliano contendo exatamente 8 elementos.

Observe também que em $D_4$ existem 6 elementos satisfazendo a equação $x^2 = e$ enquanto que em $Q_8$ existem apenas dois elementos satisfazendo a mesma equação.

EXEMPLO 11. O conjunto $G = GL(n, K)$, $n \geq 2$, de todas as matrizes $n \times n$ invertíveis com coeficientes em um corpo $K$ é um exemplo de um grupo (não abeliano), em relação a operação produto de matrizes

$$H = \{A \in GL(n, K) : \det A = 1\}$$

é um subgrupo de $GL(n, K)$ que é usualmente denotado por $H = SL(n, K)$.

EXEMPLO 12. Seja $L \supset K$ uma extensão de corpos e seja $G$ o grupo dos automorfismos de $L$, isto é, $G = \text{Aut } L$.

Pode-se provar facilmente que

$$H = \text{Aut}_K L = \{\sigma \in G : \sigma(a) = a \quad \forall\, a \in K\}$$

é um subgrupo de $G$.

EXEMPLO 13. Nesse exemplo introduziremos o grupo $A_n$ das permutações pares.

Seja $P = P(x_1, \ldots, x_n)$ o seguinte polinômio nas variáveis $x_1, \ldots, x_n$, onde $x_i x_j = x_j x_i \quad \forall\, i, j \in \{1, \ldots, n\}$,

$$P = (x_1 - x_2)(x_1 - x_3) \ldots (x_1 - x_n)(x_2 - x_3) \ldots (x_2 - x_n) \ldots (x_{n-1} - x_n)$$

o qual denotaremos por,

$$P = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Se $\sigma \in S_n$ denotaremos por $P^\sigma$ o seguinte polinômio,

$$P^\sigma = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Claramente temos $P^\sigma = \pm P$. Se $P^\sigma = P$ dizemos que a permutação $\sigma$ é uma *permutação par* e se $P^\sigma = -P$ dizemos que $\sigma$ é uma *permutação impar*.

É fácil verificar que se $\sigma, \tau \in S_n$ então $(P^\sigma)^\tau = p^{\sigma \circ \tau}$ e daí segue imediatamente que o conjunto $A_n$ de todas as permutações pares é um subgrupo de $S_n$.

Por exemplo,

$$A_3 = \{e, f, f^{-1}\}$$

onde

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

De fato, se $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ então, $P^f = (x_{f(1)} - x_{f(2)})$ $(x_{f(1)} - x_{f(3)})(x_{f(2)} - x_{f(3)}) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) \therefore P^f = P$.
Analogamente $P^{f^{-1}} = P$

Observe que o número de permutações pares coincide com o número de permutações ímpares e temos então,

$$|A_n| = \frac{n!}{2}$$

Antes de demonstrarmos o próximo resultado (Teorema de Lagrange) vamos fazer algumas considerações.

Seja $G$ um grupo e seja $H$ um subgrupo de $G$.

PROPOSIÇÃO 2. *$x, y \in G$, $x \equiv y$ (mod $H$) $\Leftrightarrow xy^{-1} \in H$ define uma relação de equivalência no conjunto $G$.*

*Demonstração.*

(i) $x \equiv x \,(\text{mod } H)$ $\forall x \in G$ pois $e = x \cdot x^{-1} \in H$.

(ii) $x \equiv y\,(\text{mod } H) \Rightarrow y \equiv x\,(\text{mod } H)$ pois se $xy^{-1} \in H$ então $yx^{-1} = (xy^{-1})^{-1} \in H$.

(iii) $x \equiv y\,(\text{mod } H)$ e $y \equiv z\,(\text{mod } H) \Rightarrow x \equiv z\,(\text{mod } H)$ pois,

$$xy^{-1} \in H \text{ e } yz^{-1} \in H \Rightarrow xz^{-1} = (xy^{-1})(yz^{-1}) \in H.$$

e isto demonstra a Proposição 2. ∎

Consideremos agora a classe de equivalência $\bar{x} = \{y \in G : y \equiv x \,(\text{mod } H)\}$.

Assim, $y \in \bar{x} \Leftrightarrow y \equiv x$ (mod $H$) $\Leftrightarrow yx^{-1} = h \in H$, p/ algum $h \in H \Leftrightarrow y = hx$ para algum $h \in H$.

Se denotarmos $Hx = \{hx : h \in H\}$ então temos que $\bar{x} = Hx$, chamada *uma classe lateral (à direita) de H em G*. Representaremos o conjunto quociente $\{\bar{x} : x \in G\}$ por $G/H$, isto é, $G/H = \{Hx : x \in G\}$ é o conjunto de todas as classes laterais (à direita) de $H$ em $G$.

Suponhamos que $G/H$ possui exatamente $n$ classes laterais, assim $G/H = \{Hx_1, Hx_2, \ldots, Hx_n\}$ onde $x_1, \ldots, x_n \in G$. Como $\{Hx_1, \ldots, Hx_n\}$ é uma partição de $G$ temos que: $Hx_i \cap Hx_j = \emptyset$ se $i \neq j$ e mais ainda $G = Hx_1 \uplus \ldots \uplus Hx_n$ (união disjunta).

Se $X$ é um conjunto finito representaremos por $|X|$ o número de elementos de $X$. Se $G$ é um grupo finito definimos *ordem de G* como sendo o número $|G|$ de elementos de $G$.

Provaremos agora o Teorema de Lagrange:

TEOREMA 1 (Lagrange). *Se G é um grupo finito e H é um subgrupo de G então $|H|$ é um divisor de $|G|$ (isto é, a ordem de H é um divisor da ordem de G).*

*Demonstração.* Definindo em $G$ a relação de equivalência $\equiv$ (mod $H$) e sendo $G$ um grupo finito segue imediatamente que o conjunto $G/H$ das classes laterais (à direita) de $G$ é finito. Digamos que

$$|G/H| = n \quad \text{e} \quad G/H = \{Hx_1, \ldots, Hx_n\}.$$

Assim,

$$G = Hx_1 \uplus Hx_2 \uplus \ldots \uplus Hx_n$$

(união disjunta) e portanto segue que,

$$|G| = |Hx_1| + |Hx_2| + \ldots + |Hx_n|$$

*Afirmação*: $|G| = n \cdot |H|$ (e isto demonstra o teorema). De fato, basta demonstrarmos que $|Hx_i| = |H|$ $\forall i$, $1 \leq i \leq n$.

Seja $\psi: H \to Hx_i$, $1 \leq i \leq n$.

$h \rightsquigarrow hx_i$

$\psi$ é evidentemente sobrejetiva, e mais se $\psi(h) = \psi(h')$ tem-se $hx_1 = h'x_i \Rightarrow h = h'$ ou seja $\psi$ é bijetiva e portanto $|H| = |Hx_i|$ qualquer que seja $i$, $1 \leq i \leq n$, como queríamos demonstrar. ■

COROLÁRIO 1. *Todo grupo finito de ordem prima é cíclico (em particular é abeliano).*

*Demonstração.* Seja $G$ um grupo e $|G| = p$ onde $p$ é um número primo. Se $x \in G$, $x \neq e$ então $\langle x \rangle$ é um subgrupo de $G$ contendo o conjunto $\{e, x\}$. Assim, pelo Teorema de Lagrange $|\langle x \rangle|$ é um divisor de $|G| = p$ e $|\langle x \rangle| > 1$. Portanto $|\langle x \rangle| = p$ e isso nos diz que $G = \langle x \rangle$. ■

COROLÁRIO 2. *Se G é um grupo tal que* $|G| \leq 5$ *então G é abeliano.*

*Demonstração.* $|G| = 1 \Rightarrow G = \{e\}, |G| = 2, 3$ ou $5 \Rightarrow |G| =$ primo $\Rightarrow$ $\Rightarrow G$ cíclico $\Rightarrow G$ abeliano. $|G| = 4$: se $\exists\, x \neq e, x \in G$ tal que $\langle x \rangle = G$ então $G$ é cíclico e portanto abeliano.

Suponhamos então que: $\forall\, x \in G,\ x \neq e$, temos $\langle x \rangle \neq G$. Ora pelo Teorema de Lagrange segue imediatamente que $|\langle x \rangle| = 2$. Assim,

$$x^2 = e,\ \forall\, x \in G,$$

Assim se $x, y \in G$ tem-se $xy = (xy)^{-1} = y^{-1} \cdot x^{-1} = y \cdot x$ ou seja $G$ é abeliano (observe que nesse caso $G$ é do tipo $\mathbb{Z}_2 \times \mathbb{Z}_2, +$).

EXERCÍCIOS

1. Prove todos os detalhes deixados por fazer nos exemplos desse parágrafo.
2. Prove que:
   a) $\mathbb{Z}(S_3) = \{e\}$
   b) $\mathbb{Z}(Q_8) = \{1, -1\}$
   c) $\mathbb{Z}(D_4) = \{e, \theta^2\}$
   d) $\mathbb{Z}(D_n) = \begin{cases} \{e\} & \text{se } n \text{ ímpar.} \\ \{e, \theta^{n/2}\} & \text{se } n \text{ par.} \end{cases}$
   e) $\mathbb{Z}(A_4) = \{e\}$.
3. Prove que $\{e, r, \theta^2, r\theta^2\}$ é um subgrupo abeliano (não cíclico) de $D_4$.
4. Prove que $\langle i, j \rangle = Q_8 = \langle j, k \rangle = \langle i, k \rangle$.
5. Descreva todas as permutações de $A_4$.
6. Calcule todos os subgrupos dos seguintes grupos:
   a) $\mathbb{Z}_2 \times \mathbb{Z}_2, +$   b) $S_3$;   c) $D_4$
   d) $Q_8$;   e) $D_6$;   f) $A_4$
7. Se $G$ é um grupo e $H \leq G$ tal que $|G/H| = n$ dizemos que *o índice de H em G é igual a n.*
   a) Calcule o índice de $H = \mathbb{Z}m \cap \mathbb{Z}n$ no grupo $G = \mathbb{Z} \cdot +$ onde $m, n$ são inteiros $\geq 1$.
   b) se $H, K \leq G$ e $|G/H| = m$ e $|G/K| = m$. Prove que $|G/H \cap K| \leq$ $\leq m \cdot n$.
   c) Calcule o índice de $A_n$ em $S_n$, e prove que $|A_n| = n!/2$.

De fato,
se $y = g^{-1}xg$ e $z = h^{-1}yh$ onde $g, h \in G$ temos $z = u^{-1}xu$ onde $u = gh$, e isto demonstra a Proposição 3. ■

Se $x \underset{G}{\sim} y$ dizemos que $x$ e $y$ são elementos conjugados em $G$. Se denotarmos $g^{-1}xg = x^g$ são válidas as seguintes propriedades:

(a) $x^e = x \quad \forall\, x \in G$
(b) $y = x^g \Rightarrow x = y^{g^{-1}} \quad \forall\, x, y, g \in G$
(c) $(x^g)^h = x^{(gh)} \quad \forall\, x, g, h \in G.$

A classe $\bar{x} = \{y : x \underset{G}{\sim} y\} = \{x^g : g \in G\}$ é chamada *classe de conjugação (em G) determinada pelo elemento $x \in G$.* Vamos denotar a classe $\bar{x}$ por $C_x$.

Se $G$ é um grupo finito e existem $n$ classes de conjugação (em $G$) com representantes $x_1, x_2, \ldots, x_n$, então

$$G = C_{x_1} \cup C_{x_2} \cup \ldots \cup C_{x_n}$$

(união disjunta) e assim chegamos a chamada equação de classes:

(1) $$|G| = |C_{x_1}| + |C_{x_2}| + \ldots + |C_{x_n}|$$

Observem que $x \in Z(G) \Leftrightarrow C_x = \{x\}$ e a equação de classes torna-se:

(2) $$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |C_{x_i}|.$$

**PROPOSIÇÃO 4.** *Seja $G$ um grupo finito e $x \in G$. Então, o índice $|G/C_{G(x)}|$ é igual ao número de elementos $|C_x|$ da classe de conjugação $C_x$. Em particular, $|C_a|$ é um divisor de $|G|\ \forall\, a \in G$.*

*Demonstração.* Seja $H = C_G(x) = \{g \in G : gx = xg\} = \{g \in G : x^g = x\}$ e seja $G/H = \{Hg : g \in G\}$ o conjunto de todas as classes laterais (à direita) de $H$ em $G$.

Pelo Teorema de Lagrange temos $|G| = |G/H|\ |H|$. Agora consideremos a função,

$$\psi:\ G/H \to C_x$$
$$Hg \rightsquigarrow x^g$$

Claramente $\psi$ é sobrejetiva, mais ainda: se $\psi(Hg_1) = \psi(Hg_2) \Rightarrow \Rightarrow x^{g_1} = x^{g_2} \Rightarrow x^{g_1 g_2^{-1}} = x \Rightarrow g_1 g_2^{-1} \in C_G(x) = H \Rightarrow Hg_1 = Hg_2$. Assim $\psi$ é bijetiva e $|G/H| = |C_x| = \dfrac{|G|}{|H|}$ como queríamos demonstrar. ■

Antes de provarmos o principal teorema desse parágrafo vamos dar a seguinte definição.

Seja $p$ um número primo e $G$ um grupo. Se $|G| = p^n$, $n \in \mathbb{N}$ dizemos que *$G$ é um $p$-grupo*. Pelo teorema de Lagrange um subgrupo de um $p$-grupo é também um $p$-grupo.

TEOREMA 2. *Se $G$ é um $p$-grupo e $|G| = p^n > 1$ então $|Z(G)| = p^m > 1$.*

*Demonstração.* Pela equação de classes temos, $|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |C_{x_i}|$ ou ainda, $|Z(G)| = |G| - \sum_{x_i \notin Z(G)} |C_{x_i}|$.

Ora $\forall\, x_i \notin Z(G)$ temos $|C_{x_i}| > 1$ e sendo $|C_{x_i}|$ um divisor de $|G| = p^n$ segue imediatamente que $|C_{x_i}| \equiv 0 \pmod p$ $\forall\, x_i \notin Z(G)$ e $|G| \equiv 0 \pmod p$ e pelo teorema de Lagrange segue que: $|Z(G)| = p^m > 1$ como queríamos demonstrar. ■

COROLÁRIO 1. *Se $p$ é um número primo e $|G| = p^2$ então $G$ é um grupo abeliano.*

*Demonstração.* Se $|G| = p^2$ temos pelo teorema anterior que $|Z(G)| = p^m > 1$. Se $|Z(G)| = p^2$ então $G = Z(G)$ e $G$ é abeliano. Suponhamos, por absurdo, que $Z(G) \subsetneq G$. Assim $\exists\, a \in G$ tal que $a \notin Z(G)$. Assim $H = C_G(a) = \{g : ga = ag\} \supseteq Z(G)$, $a \in H$, e $a \notin Z(G)$.

Portanto $H \not\supseteq Z(G)$, $|H| = p^r > |Z(G)| = p \Rightarrow |H| = p^2$ e $H = G$. Mas, isto é uma contradição pois $C(a) = G \Rightarrow a \in Z(G)$, e isto demonstra o Corolário 1. ■

Observem que provamos anteriormente que se $|G| = p$ então $G$ é cíclico e agora acabamos de demonstrar que se $|G| = p^2$ então $G$ é abeliano (observem que $\mathbb{Z}_p \times \mathbb{Z}_p$, $+$ é um exemplo de um grupo abeliano não cíclico de ordem $p^2$).

EXERCÍCIOS

1. Calcule todas as classes de conjugação para os seguintes grupos:
   a) $G = Z_5, +$
   b) $G = S_3$
   c) $G = D_4$
   d) $G = Q_8$
   e) $G = D_5$

2. Seja $G$ um grupo e $C_x$ uma classe de conjugação contendo exatamente $n$ elementos. Prove que $\exists\, H \leq G$ tal que $|G/H| = n$.

3. Seja $p$ um número primo e $G$ um $p$-grupo de ordem $p^3$. Prove que, se $G$ é não abeliano, então $|Z(G)| = p$.
4. Seja $G$ um grupo e $g \in G$. Definimos a função

$$\psi_g : G \to G$$
$$x \rightsquigarrow \psi_g(x) = x^g = g^{-1}xg$$

a) Prove que $\psi_g$ é uma função bijetiva tal que

$$\psi_g(xy) = \psi_g(x) \cdot \psi_g(y) \quad \forall x, y \in G.$$

b) se $H \leq G$ prove que $\psi_g(H) = \{g^{-1} \cdot h \cdot g : h \in H\}$ é também um subgrupo de $G$.

5. Se $G$ é um grupo finito contendo apenas duas classes de conjugação. Prove que $|G| = 2$, isto é, $G$ é um grupo cíclico de ordem 2.
6. Se $G$ é um grupo finito contendo apenas 3 classes de conjugação. Calcule as possibilidades para ordem de $G$. Mostre que no caso $|Z(G)| = 1$ existe a possibilidade $|G| = 6$. Quais são os números de elementos de cada classe?
7. Estude as possibilidades para ordem de $G$ se $G$ contém exatamente 4 classes de conjugação.
8. Determine todas as classes de conjugação dos grupos $A_4$, $D_6$ e $S_4$.

## §4 Grupos quocientes e homomorfismo de grupos

Introduzimos no parágrafo anterior a importante noção de classe de conjugação em um grupo. Nesse parágrafo vamos introduzir a noção de subgrupos normais (ou invariantes) e grupos quocientes.

Seja $G$ um grupo e seja $H \leq G$. Se $g \in G$ definimos a função $\psi_g$ (*conjugação pelo elemento* $g \in G$) por,

$$\psi_g : G \to G$$
$$x \rightsquigarrow \psi_g(x) = x^g = g^{-1}xg$$

Observe que $\psi_g(H) = \{\psi_g(h) : h \in H\} = \{h^g = g^{-1}hg : h \in H\}$ que denotaremos por $H^g$ ou $g^{-1}Hg$. É fácil provar que $H^g$ é também um subgrupo de $G$ pois:

(i) $e = e^g \in H^g$
(ii) $h_1^g, h_2^g \in H^g \Rightarrow h_1^g \cdot h_2^g = (h_1h_2)^g \in H^g$
(iii) $h^g \in H^g \Rightarrow (h^g)^{-1} = (h^{-1})^g \in H^g$.

Assim a função conjugação transforma subgrupos de $G$ em subgrupos de $G$.

Dizemos que um subgrupo $H \leq G$ é *normal* (ou *invariante*) em $G$ se $\psi_g(H) = H^g \subseteq H \quad \forall g \in G$.

Observe que

$$H^g \subseteq H \quad \forall g \in G \Rightarrow H^g = H \quad \forall g \in G.$$

Por exemplo, se $G$ é o grupo das retas do plano $\mathbb{R}^2$ com coeficientes angulares não nulos (veja Exemplo 9 do §2) e $H$ é o subgrupo de $G$ das retas de $\mathbb{R}^2$ com coeficientes angulares iguais a 1, então $H$ é um subgrupo normal de $G$. De fato, é bastante observar que: se $g(x) = ax + b$, $a \neq 0$ e $h(x) = x + c$ então $(g^{-1} \cdot h \cdot g)(x) = x + \dfrac{c}{a}$.

Se $H$ é um subgrupo normal de $G$ denotaremos por $H \trianglelefteq G$.

Claramente $\{e\}$ e $G$ são sempre subgrupos normais de $G$. Se $G$ é um grupo abeliano então qualquer subgrupo $H$ de $G$ é normal em $G$ pois, $\forall g \in G$, $H^g = \{g^{-1} \cdot h \cdot g : h \in H\} = \{h : h \in H\} = H$.

Dizemos que um grupo $G \neq \{e\}$ é *simples* se os únicos subgrupos normais de $G$ são $\{e\}$ e $G$. Assim os únicos grupos simples abelianos são os cíclicos de ordem prima.

O grupo $Q_8$ dos quaternios de ordem 8 é um exemplo de um grupo não abeliano onde qualquer de seus subgrupos é normal em $Q_8$.

PROPOSIÇAO 5. *Seja $G$ um grupo. Então,*

(a) *$N \trianglelefteq G \Leftrightarrow Ng = gN \quad \forall g \in G$ onde $gN = \{gn : n \in N\}$ é uma classe lateral (à esquerda) de $N$ em $G$.*

(b) *$N_1, N_2 \trianglelefteq G \Rightarrow N_1 \cap N_2 \trianglelefteq G$.*

(c) *$H \leq G$ e $N \trianglelefteq G \Rightarrow HN = \{h \cdot n : h \in H,\ n \in N\}$ é um subgrupo de $G$.*

(d) *$N_1 \trianglelefteq G$, $N_2 \trianglelefteq G \Rightarrow N_1 \cdot N_2 \trianglelefteq G$.*

(e) *$H \leq G$, $N \trianglelefteq G \Rightarrow H \cap N \trianglelefteq H$.*

*Demonstração.*

(a) Basta observar que $N^g = g^{-1}Ng = N \Leftrightarrow Ng = gN, \quad \forall g \in G$.

(b) Se $x \in N_1 \cap N_2$ e $g \in G$ então, $x \in N_1$ e $x \in N_2$. Assim, $x^g \in N_1^g = N_1$ e $x^g \in N_2^g = N_2$ ou seja $x^g \in N_1 \cap N_2$. Assim $(N_1 \cap N_2)^g = N_1 \cap N_2 \quad \forall g \in G$.

(c) Seja $H \leq G$ e $N \trianglelefteq G$. Vamos provar que $L = HN = \{hn : h \in H,\ n \in N\}$ é um subgrupo de $G$.

De fato,

(i) $e = e \cdot e \in HN$

(ii) $h_1m_1,\ h_2m_2 \in L \Rightarrow (h_1m_1)(h_2m_2) = h_1(h_2h_2^{-1})n_1h_2)n_2 \Rightarrow (h_1n_1)(h_2n_2) = (h_1h_2)(h_2^{-1}n_1h_2)n_2 = (h_1h_2)((n_1)^{h_2} \cdot n_2)$, e se denotarmos $h = h_1h_2, n = n_1^{h_2} \cdot n_2$ teremos $h \in H, n_1^{h_2} \in N^{h_2} = N$ e $n = n_1^{h_2} \cdot n_2 \in N$ e assim,

$$(h_1n_1)(h_2n_2) = hn \in L = HN.$$

(iii) $x = hn \in L \Rightarrow x^{-1} = n^{-1}h^{-1} = h^{-1}(h \cdot n^{-1} \cdot h^{-1})$.

Mas $h^{-1} \in H$ e $h \cdot n^{-1} \cdot h^{-1} = (n^{-1})^{h^{-1}} \in N^{h^{-1}} = N$ e portanto $x^{-1} \in L = HN$ e isto demonstra o item (c).

(d) Basta observar que $\forall g \in G$ tem-se:

$$(N_1N_2)^g = g^{-1}(N_1N_2)g = (g^{-1}N_1g)(g^{-1}N_2g) = N_1^gN_2^g$$

e como $N_1^g = N_1, N_2^g = N_2\ \forall g \in G$ segue que $(N_1N_2)^g = N_1N_2\ \forall g \in G$.

(e) Seja $x \in H \cap N$ e $h \in H$, então $x \in N$ e $x^h \in N^h = N$. Como $x, h \in H$ segue imediatamente que $x^h \in H \cap N\ \forall h \in H$ e isto demonstra o item (e). ■

Agora vamos definir a noção de grupo quociente. Seja $G$ um grupo e $N$ um subgrupo normal em $G$. Sabemos que, $x, y \in G, x \equiv y \pmod N \Leftrightarrow \Leftrightarrow xy^{-1} \in N$ define uma relação de equivalência em $G$ e $G/N = \{\bar{g} : g \in G\}$ é o conjunto quociente de $G$ por esta relação de equivalência onde $\bar{g} = Ng = \{ng : n \in N\}$ é a classe de equivalência módulo $N$ tendo $g$ como representante.

Sendo $N \trianglelefteq G$ vamos agora introduzir de modo natural uma operação no conjunto das classes $G/N$ de modo que $G/N$ seja um grupo com esta operação. Este grupo receberá o nome de *grupo quociente de G por N*.

PROPOSIÇÃO 6. *Seja $G$ um grupo e $N \trianglelefteq G$. Então, $\forall x, y \in G$, $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$ define uma operação no conjunto das classes $G/N$ e mais ainda $G/N$ é um grupo com essa operação.*

*Demonstração.* Para demonstrarmos que $\bar{x} \cdot \bar{y} = \overline{xy}$ define uma operação em $G/N$ temos que provar que a definição acima não depende da escolha dos representantes das classes. De fato, se $\bar{x} = \bar{a}$ e $\bar{y} = \bar{b}$ provaremos que $\bar{x} \cdot \bar{y} = \bar{a} \cdot \bar{b}$, isto é, $\overline{x \cdot y} = \overline{a \cdot b}$.

Para isso é suficiente provarmos que $Nxy = Nab$ ou ainda $(xy) \cdot (ab)^{-1} \in N$. Mas $xy \cdot (ab)^{-1} = xyb^{-1}a^{-1}$ e $\bar{x} = \bar{a}, \bar{y} = \bar{b}$ nos diz que $xa^{-1} \in N,\ yb^{-1} \in N$.

Se $xa^{-1} = n_1 \in N$, $yb^{-1} = n_2 \in N$ então, $(xy)(ab)^{-1} = x(n_2)a^{-1} = (n_1 a)(n_2)a^{-1} = n_1(an_2a^{-1})$ e como $n_1 \in N$ e $an_2a^{-1} \in N^{a^{-1}} = N$ segue imediatamente que,

$$(xy)(ab)^{-1} \in N$$

e nossa definição não depende da escolha dos representantes.

Agora, se $e$ é a identidade de $G$ então

(i) $\bar{e} = Ne = N$ é o elemento identidade de $G/N$ pois $\bar{e} \cdot \bar{x} = \overline{e \cdot x} = \bar{x} = \overline{x \cdot e} = \bar{x} \cdot \bar{e}$, $\forall \bar{x} \in G/N$.

(ii) $\bar{x} \cdot (\bar{y} \cdot \bar{z}) = \bar{x} \cdot \overline{(y \cdot z)} = \overline{x \cdot (y \cdot z)} = \overline{(x \cdot y) \cdot z} = \overline{(x \cdot y)} \cdot \bar{z} = (\bar{x} \cdot \bar{y}) \cdot \bar{z} \quad \forall \bar{x}, \bar{y}, \bar{z}, \in G/N$.

(iii) se $\bar{x} \in G/N$ então $\overline{x^{-1}} \cdot \bar{x} = \bar{x} \cdot \overline{x^{-1}} = \bar{e}$.

Assim $\bar{G} = G/N$ é um grupo com a operação definida pela regra $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$, $\forall \bar{x}, \bar{y} \in \bar{G}$. ■

PROPOSIÇÃO 7. *Seja $G$ um grupo e $N \trianglelefteq G$. Então,*

(a) *Se $G$ abeliano, então $\bar{G} = G/N$ é abeliano.*

(b) *Se $G$ é cíclico, então $\bar{G} = G/N$ é cíclico.*

*Demonstração.*

(a) Seja $\bar{x}, \bar{y} \in \bar{G} = G/N$. Então,

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \cdot \bar{x}$$

(b) Se $G = \langle x \rangle = \{x^m : m \in \mathbb{Z}\}$ então $\forall \bar{y} = Ny \in \bar{G} = G/N$ temos que: $y \in G = \langle x \rangle$ e assim $y = x^m$ para algum $m \in \mathbb{Z}$ e daí segue que:

$$\bar{y} = \overline{x^m} = \bar{x}^m \in \langle \bar{x} \rangle = \{\bar{x}^r / r \in \mathbb{Z}\}$$

e assim $\bar{G} = \langle \bar{x} \rangle$ como queríamos demonstrar. ■

Se $G$ é um grupo aditivo e $N \trianglelefteq G$ então denotaremos também aditivamente o grupo quociente $G/N$. Assim,

$$\bar{x} + \bar{y} = \overline{x + y},$$

onde

$$\bar{x} = N + x = \{n + x : n \in N\}$$

e

$$\bar{y} = N + y = \{n + y : n \in N\}.$$

PROPOSIÇÃO 8. *Seja $G$ um grupo, $N \trianglelefteq G$ e $\bar{G} = G/N$ o grupo quociente de $G$ por $N$. Então,*

$$\pi : G \to \bar{G}$$
$$x \rightsquigarrow \pi(x) = \bar{x}$$

*é uma função sobrejetiva (projeção canônica) tal que:*

a) $\pi(xy) = \pi(x) \cdot \pi(y) \quad \forall\, x, y \in G$

b) $N = \{x \in G : \pi(x) = \bar{e}\}$ *onde $e$ é a identidade de $G$ e $\bar{e}$ é a identidade de $\bar{G}$.*

*Demonstração.*

a) $\pi(xy) = \overline{xy} = \bar{x}\,\bar{y} = \pi(x) \cdot \pi(y) \quad \forall\, x, y \in G.$

b) $\pi(x) = \bar{e} \Leftrightarrow \bar{x} = \bar{e} \Leftrightarrow x \in N$ e isto demonstra o item b). ■

Agora vamos definir a noção de homomorfismo de grupos. Sejam $G$ e $G'$ grupos e $\psi : G \to G'$ uma função de $G$ em $G'$.

Dizemos que $\psi$ é um *homomorfismo* se $\psi(xy) = \psi(x)\,\psi(y)\ \forall\, x, y \in G$.

Observe que a projeção canônica $\pi : G \to \bar{G} = G/N$ definida na Proposição 8 é um homomorfismo de $G$ sobre $\bar{G}$.

Se o homomorfismo $\psi : G \to G'$ for bijetivo dizemos que $\psi$ é um *isomorfismo* e nesse caso dizemos que $G$ é *isomorfo* a $G'$ e denotamos por $G \simeq G'$.

Um isomorfismo $\psi : G \to G$ diz-se um *automorfismo de $G$.*

As funções $\psi_g : G \to G$ conjugação pelo elementos $g \in G$ são exemplos de automorfismos de $G$, chamados *automorfismos internos* de $G$. Denotaremos por Aut $G$ o conjunto dos automorfismos de $G$ e Inn $G$ o conjunto dos automorfismos internos de $G$.

PROPOSIÇÃO 9. *Se $G$ é um grupo e $f_1, f_2 \in Aut\ G$ então:*

a) $f_1 \circ f_2 \in Aut\ G$

b) $f_1^{-1} \in Aut\ G$, *onde $f_1^{-1}$ é a função inversa de $f_1$.*

*Demonstração.*

a) $(f_1 \circ f_2)(xy) = f_1(f_2(xy)) = f_1(f_2(x) \cdot f_2(y)) = f_1(f_2(x) \cdot f_1(f_2(y)) = (f_1 \circ f_2)(x) \cdot (f_1 \circ f_2)(y)\ \forall\, x, y \in G$, e como a composição $f_1 \circ f_2$ de funções bijetivas é também bijetiva temos $f_1 \circ f_2 \in$ Aut $G$.

b) Se $f_1 \in$ Aut $G$ então $\forall\, x', y' \in G$ existem $x, y \in G$ tais que $x' = f_1(x)$ e $y' = f_1(y)$.

Assim, se $h = f_1^{-1}$ temos,

$$h(x'y') = h(f_1(x) \cdot f_2(x)) = h(f_1(xy)) = (h \circ f_1)(xy) = xy = h(x') \cdot h(y'),$$

e isto demonstra que $f_1^{-1} = h \in \text{Aut } G$. ■

COROLÁRIO 1. *Se G é um grupo então Aut G é também um grupo com a operação de composição de funções.*

*Demonstração.* Usando a proposição anterior é bastante observar que $e = I_G : G \to G$ é um automorfismo de $G$ e que a composição de funções é associativa. ■

PROPOSIÇÃO 10. *Se G é um grupo então* Inn *G é um subgrupo normal de Aut G.*

*Demonstração.* Primeiramente, se $g_1, g_2 \in G$, então

$$\psi_{g_1} \circ \psi_{g_2} = \psi_{g_2 g_1} \text{ pois } \psi_{g_2 g_1}(x) = $$
$$= (g_2 g_1)^{-1} x (g_2 g_1) = g_1^{-1}(g_2^{-1} x g_2) g_1 \quad \forall x \in G.$$

Assim Inn$(G)$ é um subconjunto fechado em relação a composição de funções. Como $\psi_e = I_e \in \text{Inn}(G)$ e $(\psi_g)^{-1} = \psi_{g^{-1}} \in \text{Inn}(G)$ $\forall g \in G$ segue imediatamente que Inn $G$ é um subgrupo de $G$.

Agora se $g \in G$, $\sigma \in \text{Aut } G$, então

$$(\sigma^{-1} \circ \psi_g \circ \sigma)(x) = \sigma^{-1}(g^{-1} \cdot \sigma(x) \cdot g) = (\sigma^{-1}(g))^{-1} x \sigma^{-1}(g) =$$
$$= \psi_{\sigma^{-1}(g)}(x) \quad \forall x \in G,$$

ou seja, $\sigma^{-1} \cdot \psi_g \cdot \sigma \in \text{Inn}(G)$ $\forall \sigma \in \text{Aut } G$, $\forall g \in G$, e isto demonstra a Proposição 10. ■

TEOREMA 3 (1.º Teorema de homomorfismo). *Sejam G e G′ grupos com identidades e e e′ respectivamente e $\psi : G \to G'$ um homomorfismo. Então*

a) *Im $\psi = \psi(G) = \{\psi(g) : g \in G\}$ é um subgrupo de $G'$.*

b) *$N(\psi) = \{g \in G : \psi(g) = e'\}$ é um subgrupo normal de G (chamado de* núcleo *do homomorfismo) e mais,*

$$\psi \text{ é injetiva} \Leftrightarrow N(\psi) = \{e\}$$

c) *$G/N(\psi) \simeq$ Im $\psi$.*

*Demonstração.*

a) Primeiramente, (i) $e' = \psi(e) \in \text{Im}\ \psi$ pois $e \cdot e = e \Rightarrow \psi(e) \cdot \psi(e) \Rightarrow$ $\Rightarrow \psi(e) = e' \in \text{Im}\ \psi$, logo $\text{Im}\ \psi \neq \varnothing$

(ii) $\psi(g_1), \psi(g_2) \in \text{Im}\ \psi \Rightarrow \psi(g_1) \cdot \psi(g_2)^{-1} = \psi(g_1 g_2^{-1}) \in \text{Im}\ \psi\ \forall\ g \in G.$

e isto demonstra o item a), pela proposição 1 da pág. 126.

b) (i) $e \in N(\psi)$ pois $\psi(e) = e'$

(ii) $g_1, g_2 \in N(\psi) \Rightarrow \psi(g_1 g_2) = \psi(g_1) \cdot \psi(g_2) = e' \cdot e' = e' \Rightarrow$ $\Rightarrow g_1 g_2 \in N(\psi)$.

(iii) $g \in N(\psi) \Rightarrow \psi(g^{-1}) = \psi(g)^{-1} = e'^{-1} = e' \Rightarrow g^{-1} \in N(\psi)$.

Agora se $n \in N(\psi)$ e $g \in G$ temos,

$$\psi(g^{-1} \cdot n \cdot g) = \psi(g)^{-1} \cdot \psi(n) \cdot \psi(g) = \psi(g)^{-1} \cdot e' \cdot \psi(g) = e',$$

ou seja, $g^{-1} \cdot n \cdot g \in N(\psi)$. $\forall\ n \in N(\psi)$, $\forall\ g \in G$.

Assim $N(\psi)$ é um subgrupo normal de $G$.

Agora, se $x, y \in G$ $\psi(x) = \psi(y) \Leftrightarrow \psi(x) \cdot \psi(y)^{-1} = e' \Leftrightarrow \psi(xy^{-1}) =$ $= e' \Leftrightarrow xy^{-1} \in N(\psi)$, e daí segue imediatamente o item b) do Teorema 3.

c) Seja $\bar{G} = G/N(\psi)$ e $N = N(\psi) \trianglelefteq G$. Vamos definir

$$\bar{\psi}\colon \bar{G} \to \text{Im}(\psi).$$
$$\bar{g} \rightsquigarrow \psi(g)$$

Primeiramente $\bar{\psi}$ está bem definida pois,

$$\bar{g} = \bar{h} \Rightarrow gh^{-1} \in N(\psi) \Rightarrow \psi(gh^{-1}) = e' \Rightarrow \psi(g) = \psi(h)$$

Agora, $\text{Im}\ \bar{\psi} = \text{Im}\ \psi$ e portanto a função é sobrejetiva.

Se $\bar{x}, \bar{y} \in \bar{G} = G/N$ temos,

$$\overline{\psi}(\bar{x}\bar{y}) = \overline{\psi}(\overline{xy}) = \psi(xy) = \psi(x) \cdot \psi(y) = \overline{\psi}(\bar{x}) \cdot \overline{\psi}(\bar{y})$$

ou seja, $\psi$ é um homomorfismo sobjetivo.

Mais ainda,

$$\bar{\psi}(\bar{x}) = e' \Leftrightarrow \psi(x) = e' \Leftrightarrow x \in N \Leftrightarrow \bar{x} = \bar{e}.$$

Daí segue que $N(\overline{\psi}) = \{\bar{e}\}$ e $\overline{\psi}$ é injetiva. Assim $\overline{\psi}$ é um isomorfismo de $\bar{G}$ sobre $\text{Im}(\psi)$ e portanto $\overline{G} \simeq \text{Im}\ \psi$, e isto demonstra o Teorema 3. ■

COROLÁRIO 1. *Seja $G$ um grupo finito e $\psi\colon G \to G'$ um homomorfismo de grupos. Então,*

(a) *$|\psi(G)|$ é um divisor de $|G|$*

(b) *se $G$ é um p-grupo então $\psi(G) = \text{Im}\ \psi$ é também um p-grupo.*

*Demonstração.* Basta observar que $G/N \simeq \psi(G) \Rightarrow |G/N| = |\psi(G)|$ onde $N = N(\psi)$ é o núcleo de $\psi$. ■

COROLÁRIO 2. *Seja G um grupo e Z(G) o centro do grupo G. Então,* $\text{Inn}\, G \simeq G/Z(G)$.

*Demonstração.* Basta observar que a função, $\psi\colon G \to \text{Inn}\, G$, $g \rightsquigarrow \psi_{g^{-1}}$ é um homomorfismo tal que: $\text{Im}(\psi) = \text{Inn}\, G$ e $N(\psi) = Z(G)$.
De fato, $\psi$ é um homomorfismo pois $\psi(gh) = \psi_{(gh)^{-1}}$ e $\psi_{(gh)^{-1}}(x) = (gh) \cdot x \cdot (h^{-1}g^{-1}) = g(h \cdot x \cdot h^{-1}) \cdot g^{-1} \Rightarrow \psi_{(gh)^{-1}}(x) = \psi_{g^{-1}}(\psi_{h^{-1}}(x))$, $\forall\, x \in G$.

Assim, $\psi(gh) = \psi(g) \cdot \psi(h)$ $\forall\, g, h \in G$. Agora, $\text{Im}(\psi) = \text{Inn}(G)$ e $N(\psi) = \{g \in G : \psi_{g^{-1}} = I_G\}$ $\therefore N(\psi) = \{g \in G : g \cdot x \cdot g^{-1} = x\ \forall\, x \in G\} = \{g \in G : gx = xg\ \forall\, x \in G\}$ $\therefore N(\psi) = Z(G)$. E isto demonstra o Corolário 2. ■

TEOREMA 4 (Teorema da Representação). *Seja G um grupo e H um subgrupo de G de índice* $[G : H] = n$. *Então,* $\exists\, N \subseteq H, | N \trianglelefteq G$ *tal que G/N é um grupo isomorfo a um subgrupo do grupo* $S_n$.

*Mais ainda, N é o "maior" subgrupo normal em G que está contido em H.*

COROLÁRIO 1 (Teorema de Cayley). *Se G é um grupo de ordem* $|G| = n$ *então G é isomorfo a um subgrupo do grupo* $S_n$.

*Demonstração do Corolário* 1 – Basta fazer $H = \{e\}$ no enunciado do Teorema 4. ■

*Demonstração do Teorema* 4 – Seja $S = G/H = \{Hx_1, Hx_2, \ldots, Hx_n\}$. e $\mathscr{P}(S)$ o grupo de permutações do conjunto $S$. Seja a seguinte função,

$$\psi\colon G \to \mathscr{P}(S) \quad \text{onde} \quad \psi(g)\colon S \to S$$
$$g \rightsquigarrow \psi(g) \qquad\qquad Hx_i \rightsquigarrow Hx_i g^{-1}$$

Primeiramente, se $g \in G$,

$$\psi(g)(Hx_i) = \psi(g)(Hx_j) \Leftrightarrow Hx_i g^{-1} = Hx_j g^{-1} \Leftrightarrow Hx_i = Hx_j \Rightarrow \psi(g)$$

é injetiva e $|S| = n \Rightarrow \psi(g) \in \mathscr{P}(S)$.

Assim, $\psi(g) \in \mathscr{P}(S)\ \ \forall\, g \in G$.

Agora, $\psi(gh)(Hx_i) = Hx_i(gh)^{-1} = Hx_ih^{-1}g^{-1} = (\psi(g) \circ \psi(h))(Hx_i)\ \forall g, h \in G$ e $\forall Hx_i \in S$. Portanto $\psi$ é um homomorfismo $\psi : G \to \mathscr{P}(S)$.

Vamos calcular o núcleo de $\psi$:

$$N(\psi) = \{g \in G : \psi(g) = I_S\} = \{g \in G : Hx_ig^{-1} = Hx_i\ \forall i = 1, 2, \ldots, n\}$$

Assim, $g \in N(\psi) \Leftrightarrow Hx_ig^{-1} = Hx_i\ \forall i = 1, \ldots, n \Leftrightarrow Hx_i = Hx_ig\ \forall i = 1, \ldots, n \Leftrightarrow H = H(x_igx_i^{-1})\ \forall i = 1, \ldots, n \Leftrightarrow x_igx_i^{-1} \in H\ \forall i = 1, \ldots, n \Leftrightarrow g \in x_i^{-1}Hx_i = H^{x_i}\ \forall i = 1, 2, \ldots, n$.

Ora como $G = Hx_i \cup \ldots \cup Hx_n$ (união disjunta) e como $H^{hx_i} = H^{x_i}\ \forall h \in H$ segue imediatamente que:

$$g \in N(\psi) \Leftrightarrow g \in H^x\quad \forall x \in G \Leftrightarrow g \in \bigcap_{x \in G} H^x.$$

Portanto, $N(\psi) = \bigcap_{x \in G} H^x$.

Se $N = \bigcap_{x \in G} H^x$ então $N \trianglelefteq G$ pois $N = N(\psi)$ e também $H = H^e \supseteq N$.

Agora, se $L \trianglelefteq G$ e $L \subseteq H$ segue que: $L^x = L \subseteq H^x\ \forall\, x \in G$ e daí teremos $L \subseteq N = \bigcap_{x \in G} H^x$. Portanto, $N = \bigcap_{x \in G} H^x$ é o "maior" subgrupo normal de $G$ contido em $H$.

Ora como o grupo $\mathscr{P}(S) \simeq S_n$ o teorema segue imediatamente. ■

COROLÁRIO 2. *Seja $G$ um grupo finito e $H \leq G$ tal que $[G : H] = n$. Seja $N = \bigcap_{x \in G} H^x$ o maior subgrupo normal em $G$ contido em $H$.*

*Se $|G|$ não divide $n!$ então $N \neq \{e\}$.*

*Demonstração.* Basta observar que pelo Teorema de Lagrange e pelo teorema anterior temos que $|G/N|$ é um divisor de $n!$. ■

COROLÁRIO 3. *Seja $G$ um grupo finito e $p$ o menor divisor de $|G|$. Se existe $H \leq G$ tal que $[G : H] = p$ então $H \trianglelefteq G$.*

*Demonstração.* Se $N = \bigcap_{x \in G} H^x$ então pelo Teorema de Lagrange e pelo teorema anterior temos que $|G/N|$ é um divisor de $p!$.

Ora como $p$ é o menor primo divisor de $|G|$ então pelo Teorema de Lagrange $p$ é o menor primo divisor de $|G/N|$. Assim a única possibilidade de termos $|G/N|$ dividindo $p!$ é $|G/N| = p$.

Mas $N \subseteq H \subseteq G$ e $[G:H] = [G:N] = p$ nos diz que $|N| = |H|$, ou seja, $N = H \trianglelefteq G$, como queríamos demonstrar. ■

COROLÁRIO 4. *Seja $G$ um grupo e $H \leq G$ tal que $[G:H] = 2$, então $H \trianglelefteq G$. Em particular, $A_n \trianglelefteq S_n$.* ■

COROLÁRIO 5. *Todo subgrupo $H$ de índice $p$ primo em um $p$-grupo $G$ é normal em $G$.*

*Demonstração.* Segue imediatamente do Corolário 3. ■

COROLÁRIO 6. *Se $G$ é um grupo simples e $H$ é um subgrupo de $G$ tal que $[G:H] = n > 1$. Então $G$ é isomorfo a um subgrupo do grupo $S_n$. Em particular um grupo simples infinito não contém subgrupo próprio de índice finito.*

*Demonstração.* Se $N = \bigcap_{x \in G} H^x \trianglelefteq G$ e $H \neq G$, $G$ simples então $N = \{e\}$ e nesse caso $G/N \simeq G$ e o corolário segue imediatamente do Teorema 4. ■

TEOREMA 5 (Teorema da Correspondência). *Sejam $G$ e $G'$ grupos e $\psi : G \to G'$ um homomorfismo sobrejetivo tal que $N = N(\psi)$. Então:*

(a) *$\forall\, H \leq G$ tem-se $H' = \psi(H) = \{\psi(h) : h \in H\} \leq G'$. Mais ainda $H \trianglelefteq G \Rightarrow H' \trianglelefteq G'$.*

(b) *$\forall\, H' \leq G'$ $\exists$ único $H = \psi^{-1}(H') = \{g \in G : \psi(g) \in H'\} \supseteq N$, $H \leq G$ tal que $\psi(H) = H'$.*

*Mais ainda $H' \trianglelefteq G' \Rightarrow H \trianglelefteq G$.*

COROLÁRIO 1. *Seja $G$ um grupo e $N \trianglelefteq G$. Então, todo subgrupo do grupo quociente $\overline{G} = G/N$ é do tipo $\overline{H} = H/N$ onde $H$ é o único subgrupo de $G$ contendo $N$ tal que $\pi(H) = \overline{H}$ onde $\pi : G \to \overline{G} = \overline{G}/N$ é a projeção canônica ($H$ recebe o nome de pré-imagem de $H$ em $G$). Mais ainda,*

$$\overline{H} \trianglelefteq \overline{G} \Leftrightarrow H \trianglelefteq G.$$

*Demonstração do Corolário* 1. Basta considerar na parte (b) do Teorema 5

$\psi = \pi : G \to \overline{G} = G' = G/N$. ■

*Demonstração do Teorema* 5.

(a) Seja $H \leq G$.

Considerando $\hat{\psi} = \psi|_H : H \to G'$ a restrição de $\psi$ ao subgrupo $H$ de $G$ temos claramente que $\hat{\psi} : H \to G'$ é ainda um homomorfismo e pelo 1.º teorema de homomorfismo segue que $\psi(H) = Im\,\hat{\psi} \trianglelefteq G'$.

Seja $H \trianglelefteq G$ e $H' = \psi(H)$. Vamos provar que $H' \trianglelefteq G'$. De fato, se $g' \in G' = Im\ \psi$ temos que $g' = \psi(g)$ para algum $g \in G$. Assim, $\forall\, h' \in H' = \psi(H)\ \exists\, h \in H$ tal que $\psi(h) = h'$ e $\forall\, g' \in G'\ \exists\, g' \in G$ tal que $g' = \psi(g)$. Daí segue que:

$$g'^{-1} \cdot h' \cdot g' = \psi(g)^{-1} \cdot \psi(h) \cdot \psi(g) = \psi(g^{-1} \cdot h \cdot g)$$

ora $H \trianglelefteq G$ implica que $g^{-1} \cdot h \cdot g \in H^g = H$ e daí temos,

$$g'^{-1} \cdot h' \cdot g' = \psi(g^{-1} \cdot h \cdot g) \in \psi(H) = H', \forall\, g' \in G', \forall\, h' \in H'$$

ou seja $H \trianglelefteq G \Rightarrow H' \trianglelefteq G' = \psi(G)$.

(b) Seja $H' \leq G'$ e $H = \psi^{-1}(H') = \{g \in G : \psi(g) \in H'\}$.

Ora como $e' \in H'$ segue imediatamente que

$$N = N(\psi) = \{g \in G : \psi(g) = e\} \subseteq H = \psi^{-1}(H').$$

Claramente temos $\psi(H) = \psi(\psi^{-1}(H')) \subseteq H'$. Vamos provar agora que $\psi(H) = H'$. De fato, se $h' \in H'$ então $\exists\, x \in G : \psi(x) = h'$ pois $\psi$ é sobrejetiva. Então $x \in \psi^{-1}(H') = H$ e mais $h' = \psi(x) \in \psi(H)$ e isto prova que $\psi(H) = H'$.

Se $H' \trianglelefteq G'$, $H = \psi^{-1}(H') \trianglelefteq G = \psi^{-1}(G')$ pois, $\forall\, g \in G, \forall\, h \in H$ temos

$$\psi(g^{-1} \cdot h \cdot g) = \psi(g)^{-1} \cdot \psi(h) \cdot \psi(g) \in H'^{\psi(g)} = H'$$

e portanto $g^{-1} \cdot h \cdot g \in H = \psi^{-1}(H')$.

Agora se $H' \leq G'$ e $L \leq G$, $L \supseteq N$ tal que $\psi(L) = H'$ então $L = H = \psi^{-1}(H')$, pois $\psi(L) = H'$ nos diz de imediato que $L \subseteq H = \psi^{-1}(H')$. Por outro lado, se $h \in H = \psi^{-1}(H')$ temos que $\psi(h) \in H' = \psi(L)$, isto é, $\exists \ell \in L$ tal que $\psi(h) = \psi(\ell)$ e daí temos: $\psi(h\ell^{-1}) = e'$ ou seja $h\ell^{-1} \in N \subseteq L$ ou ainda, $h\ell^{-1} \in L$ e portanto $h \in L \cdot \ell = L$, e isto demonstra a unicidade de $H \supseteq N$ tal que $\psi(H) = H'$. ■

Antes de encerrarmos esse parágrafo vamos demonstrar o Teorema de Cauchy e enunciar, sem demonstração, o Teorema de Sylow. Esses Teoremas foram os primeiros resultados da Teoria dos grupos relativo ao problema da Existência de subgrupos em grupos Finitos.

TEOREMA 6 (Cauchy-1842). *Seja p um divisor primo da ordem de um grupo finito G. Então* $\exists\, a \in G$ *tal que a ordem de a é igual a p.*

*Demonstração.* Vamos demonstrar por indução sobre $|G|$. Se $|G| = 1$ o teorema é verdadeiro pois não existe primo dividindo $|G| = 1$. Vamos então assumir o teorema verdadeiro para todos os grupos $L$ tais que $1 \leq |L| < |G|$.

*Caso* 1 – $G$ grupo cíclico.

Seja $G = \langle x \rangle$ e seja $p$ um divisor primo de $|G|$.

Nesse caso sabemos que $\mathcal{O}(x) = p^r \cdot m$ onde $r \geq 1$ e $a = x^{p^{r-1} \cdot m}$ é tal que $a^p = e, a \neq e$ como queríamos demonstrar.

*Caso* 2 – $G$ abeliano não cíclico.

Seja $p$ um divisor primo de $|G|$ e seja $x \in G$ $x \neq e$. Se $p$ divide $|\langle x \rangle|$ então pelo caso anterior $\exists\, a \in \langle x \rangle$ tal que $\mathcal{O}(a) = p$ e o teorema está provado.

Suponhamos então que $p$ não divide $|N|$ onde $N = \langle x \rangle$. Pelo Teorema de Lagrange temos que $p$ divide a ordem do grupo quociente $L = G/N$ (observe que $N \trianglelefteq G$ pois $G$ é abeliano). Como $|L| < |G|$ temos pela hipótese de indução que $\exists\, \bar{g} \in L$ tal que $\bar{g} \neq \bar{e}$ e $\bar{g}^p = \bar{e}$ ou seja $\bar{g}^p = \bar{e}$ ou ainda $g \notin N$, $g^p \in N$. Agora se $|N| = n$ temos então que $(g^p)^n = g^{pn} = e$, portanto $p$ divide $|\langle g \rangle|$ e novamente pelo caso 1 $\exists\, a \in \langle g \rangle$ tal que $\mathcal{O}(a) = p$ e o teorema está provado.

*Caso* 3 – $G$ não abeliano.

Assim $Z = Z(G) \neq G$. Se $p$ divide $|Z|$ temos o teorema provado pelo Caso 2. Assim podemos assumir que $p$ não divide $|Z|$.

Pela equação de classes temos,

$$|G| = |Z| + \sum_{x_i \notin Z(G)} [G : C_G(x_i)]$$

Como $p$ divide $|G|$ e $p$ não divide $|Z|$ segue que $\exists\, x_i \notin Z(G)$ tal que $p$ não divide $[G : C_G(x_i)]$.

Portanto $p$ divide $|H|$ onde $H = C_G(x_i) \neq G$. Como $|H| < |G|$ pela hipótese de indução temos que $\exists\, a \in H$ tal que $\mathcal{O}(a) = p$ e o teorema está demonstrado. ■

COROLÁRIO 1. *Se $G$ é um grupo de ordem 6 então ou $G$ é cíclico ou $G \simeq S_3$.*

*Demonstração.* Seja $G$ um grupo e $|G| = 6$, então pelo teorema de Cauchy $\exists\, x, y \in G$ tais que, $\mathcal{O}(x) = 2$, $\mathcal{O}(y) = 3$. Se $N = \langle y \rangle = \{e, y, y^2\}$ segue que $[G : N] = 2$ e portanto $N \trianglelefteq G$. Em particular $x^{-1} \cdot y \cdot x \in N = \{e, y, y^2\}$ e daí segue que ou $x^{-1} \cdot y \cdot x = y$ (e nesse caso $xy = yx$) ou $x^{-1} \cdot y \cdot x = y^{-1}$ (e nesse caso $G = \{c, x, y, y^2, xy, xy^2\}$ onde $yx = xy^{-1}$).

No primeiro caso se $a = x \cdot y$ é fácil ver que $\mathcal{O}(a) = 6$ e $G = \langle a \rangle$ é cíclico. No segundo caso a correspondência: $r \leftrightarrow x$ e $\theta \leftrightarrow y$, define um isomorfismo entre, $D_3 \simeq S_3$ e $G$ pois $\theta r = r\theta^{-1}$ e $yx = xy^{-1}$.

Observe que já classificamos todos os grupos de ordem até 6. Os grupos de ordem 1, 2, 3 e 5 são grupos cíclicos. Os grupos de ordem 4 são ou abelianos cíclicos (isomorfos à $\mathbb{Z}_4, +$) ou são abelianos isomorfos à $\mathbb{Z}_2 \times \mathbb{Z}_2, +$. Os grupos de ordem 6 são de dois tipos, ou abelianos cíclicos (isomorfos a $\mathbb{Z}_6, +$) ou não abelianos isomorfos à $S_3$.

O problema de classificar todos os grupos finitos é o problema central da Teoria dos grupos finitos e é extremamente difícil. Apenas para dar uma idéia, podemos informar que existem 14 tipos distintos de grupos de ordem 16 sendo 5 abelianos (apenas 1 cíclico) e 9 não abelianos. Os grupos de ordem 8 e 12 são mais tratáveis do que àqueles de ordem 16 e poderiam mesmo serem aqui apresentados, mas nos restringiremos à mais uma informação através da seguinte proposição.

PROPOSIÇÃO 11. *Seja $G$ um grupo de ordem 8 então $G$ é isomorfo à um dos seguintes grupos:*

$$\text{(A) } G \text{ Abeliano: } \begin{cases} (1)\ G \simeq \mathbb{Z}_8, + \\ (2)\ G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2, + \\ (3)\ G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, + \end{cases}$$

$$\text{(B) } G \text{ Não Abeliano: } \begin{cases} (4)\ G \simeq D_4 \text{ (Dihedral)} \\ (5)\ G \simeq Q_8 \text{ (Quaternios)} \end{cases}$$

Para concluir o parágrafo 4 vamos enunciar, sem demonstração, o Teorema de Sylow, cuja demonstração é em geral apresentada em um primeiro curso de Álgebra do Mestrado.

TEOREMA 7 (Sylow-1872). *Seja* $G$ *um grupo finito,* $|G| = p^\alpha \cdot m$ *onde* $M.D.C.\{p, m\} = 1$, *e* $\alpha \geq 1$. *Então,*

a) $\forall r,\ 1 \leq r \leq \alpha\ \exists H \leq G$ *tal que* $|H| = p^r$.

b) *Quaisquer dois subgrupos* $H_1$ *e* $H_2$ *de* $G$ *de ordem igual a* $p^\alpha$ *são conjugados em* $G$ (*i.e.,* $\exists\, g \in G$ *tal que* $H_1^g = H_2$).

c) *O número* $n_p$ *de subgrupos de* $G$ *de ordem* $p^\alpha$ *é do tipo* $n_p = kp + 1$ *onde* $k \in \mathbb{N}$, *e* $n_p \mid |G|$.

(*os subgrupos de* $G$ *de ordem* $p^\alpha$ *são chamados de* p-Sylow subgrupos *de* $G$)

EXERCÍCIOS

1. Calcule todos os subgrupos normais dos seguintes grupos: $S_3, D_4, Q_8, A_4$ e $S_4$.
2. Mostre com um contra-exemplo que: $N_1 \trianglelefteq G_1,\ N_2 \trianglelefteq G_2,\ N_1 \simeq N_2$ e $\frac{G_1}{N_1} \simeq \frac{G_2}{N_2}$ não implica que $G_1 \simeq G_2$.
3. Calcule Aut $G$ para os seguintes grupos $G$:
   a) $G = \mathbb{Z}_2 \times \mathbb{Z}_2, +$
   b) $G = \mathbb{Z}_4, +$
   c) $G = \mathbb{Z}_8, +$
   d) $G = \mathbb{Z}_4 \times \mathbb{Z}_2, +$
   e) $G = \mathbb{Z}_6, +$
   f) $G = S_3$
   g) $G = D_4$
   h) $G = Q_8$
   i) $G = A_4$
   j) $G = S_4$
4. Prove que quocientes e subgrupos de grupos abelianos são ainda grupos abelianos.
5. Prove que quocientes e subgrupos de p-grupos são ainda p-grupos.
6. Seja $S_3 = \{e, x, y, y^2, xy, xy^2\} = G$ onde $\mathcal{O}(x) = 2$ e $\mathcal{O}(y) = 3$. Se $N = \{e, y, y^2\}$ então $N$ é abeliano, $G/N$ é abeliano mas $G$ não é abeliano.
7. Seja $G$ um grupo e $N \leq G$. Prove que, se $G/N$ e $N$ são $p$-grupos (para algum primo $p$) então $G$ é também um $p$-grupo.

8. Prove que se $G \neq \{e\}$ é um grupo simples abeliano então $G$ é um grupo cíclico de ordem prima.

9. Seja $G$ um grupo e $H$ um subgrupo de $G$.
Se $N_G(H) = \{g \in G : H^g = H\}$ então prove que:
a) $N_G(H)$ é um subgrupo de $G$ contendo $H$ e $Z(G)$.
b) $H \trianglelefteq N_G(H)$ e se $L$ é um subgrupo de $G$, $L \supseteq H$ tal que $H \leq L$ então $L \subseteq N_G(H)$.
c) O índice $[G : N_G(H)]$ é igual ao número de subgrupos $H^g$ conjugados ao grupo $H$. (considere aqui $G$ um grupo finito).
d) $H \trianglelefteq G \Leftrightarrow N_G(H) = G$.
($N_G(H)$ é chamado de *normalizador de H em G*)

10. Sejam $N_1$, $N_2$ subgrupos normais de um grupo $G$ tais que: $G = N_1 N_2$ e $N_1 \cap N_2 = \{e\}$.
Prove que: se $g \in G$ existe únicos $n_1 \in N_1$, $n_2 \in N_2$ tais que: $g = n_1 n_2$.

11. Um subgrupo $K$ de um grupo $G$ diz-se *característico em G* se $\forall \alpha \in \text{Aut } G$ tem-se $K^\alpha = \{\alpha(k) : k \in K\} = K$. Prove que:
a) se $K \leq N \leq G$, $K$ característico em $N$ e $N \trianglelefteq G$ então $K \trianglelefteq G$.
b) se $K \leq L \leq G$ e $K$ característico em $L$ e $L$ característico em $G$ então $K$ é também característico em $G$.
c) de um contra-exemplo mostrando que:
$$N_1 \trianglelefteq N_2 \quad \text{e} \quad N_2 \trianglelefteq G \not\Rightarrow N_1 \trianglelefteq G.$$
d) se $K$ é característico em $G$ então $K \trianglelefteq G$.

12. Seja $G$ um grupo abeliano finito e seja $n$ um inteiro $\geq 1$ tal que M.D.C.$\{n, |G|\} = 1$. Prove que:
$$\begin{aligned} \psi : G &\to G \\ x &\rightsquigarrow x^n \end{aligned}$$
é um automorfismo de $G$.

13. Sejam $M, N \trianglelefteq G$. Prove que:
$$MN/N \simeq M/M \cap N$$
*Sugestão*: Considere o homomorfismo definido por:
$\psi : M \to MN/N$, $m \rightsquigarrow Nm$ e mostre que $\psi$ é sobrejetivo e mais $N(\psi) = M \cap N$.

14. Seja $G$ um grupo e seja $C$ o seguinte subconjunto de $G$:

$$C = \{[x, y] = x^{-1} \cdot y^{-1} \cdot x \cdot y : x, y \in G\}.$$

($[x, y]$ chama-se um comutador de $G$ e $C$ é o conjunto de todos os comutadores de $G$).

Vamos definir $G'$ como o subgrupo gerado por $C$, isto é, $G' = \langle C \rangle$ é o menor subgrupo de $G$ contendo $C$. Prove que:

a) $G$ abeliano $\Leftrightarrow G' = \{e\}$.

b) $G'$ é um subgrupo característico em $G$.

c) $G/G'$ é um grupo abeliano.

d) se $N \trianglelefteq G$ e $G/N$ é abeliano então $N \supseteq G'$.

e) se $H \leq G$ e $H \supseteq G'$ então $H \trianglelefteq G$.

15. Se $G$ é um grupo tal que $|G| \geq 3$ então $|\text{Aut}\, G| \geq 2$.

16. Seja $G$ um grupo tal que $|G| = 2 \cdot p$ onde $p$ é um número primo. Então $\exists\, H \trianglelefteq G$ tal que $|H| = p$.

17. Seja $G$ um grupo tal que $|G| = p \cdot q$ onde $p$ e $q$ são primos. Prove que:

a) Se $G$ é abeliano e $p \neq q$ então $G$ é cíclico.

b) Se $p < q$ então $\exists$ subgrupo $Q \trianglelefteq G$ tal que $|Q| = q$.

18. Seja $G$ um grupo de ordem 15. Prove que $G$ é cíclico.

19. Seja $G$ um grupo não abeliano de ordem 10. Prove que $G \simeq D_5$.

20. Seja $G$ um grupo tal que $G/Z(G)$ é cíclico. Prove que $G$ é abeliano.

21. Prove que se $G$ é um grupo de ordem 28 então $G$ possui um subgrupo normal de ordem 7.

22. Seja $G$ um grupo tal que $\exists\, H \leq G$ onde $[G : H] = n$. Prove que então $\exists\, N \trianglelefteq G$ tal que $[G : N] < \infty$.

23. Seja $G$ um grupo e $H \leq G$.

a) Prove que $C_G(H) = \{g \in G : gh = hg \ \forall\, h \in H\}$ é um subgrupo de $G$ contendo $Z(G)$ e contido em $N_G(H)$.

b) Prove que $C_G(H) \trianglelefteq N_G(H)$.

c) Prove que $N_G(H)/C_G(H)$ é isomorfo a um subgrupo do grupo $\text{Aut}\,(H)$.

(*Sugestão*: considere o homomorfismo:

$$\psi : N_G(H) \to \text{Aut}(H) \quad \text{onde} \quad \psi_g : H \to H$$
$$g \rightsquigarrow \psi_g \qquad\qquad\qquad h \rightsquigarrow h^g = g^{-1} \cdot h \cdot g$$

24. Seja $G = \mathbb{Q}, +$ e $H = \mathbb{Z}, +$. Assim $H \trianglelefteq G$. Considere o grupo $\bar{G} = G/H$ e prove que $\bar{G}$ é um grupo abeliano infinito tal que todos os seus elementos (distintos da identidade) possuem ordem finita.
25. No exemplo anterior descreva o subgrupo de $\bar{G}$ contendo todos os elementos de ordem potencia de um dado número primo.
26. Seja $G$ um grupo e $M \neq G$ um subgrupo maximal normal em $G$ (isto é, não existe subgrupo $N \trianglelefteq G$ tal que $M \subsetneqq N \subsetneqq G$). Então prove que $G/M$ é um grupo simples.
27. Seja $P$ um p-sylow subgrupo de um grupo finito $G$ e seja $N = N_G(P)$. Prove que o grupo $N/P$ não possui elementos (distintos da identidade) com ordem potencia do primo $p$.
28. Seja $G$ um grupo finito e $P$ um p-sylow subgrupo de $G$. Se $N \trianglelefteq G$, prove que $P \cap N$ é um p-sylow subgrupo de $N$ e $PN/N$ é um p-sylow subgrupo de $G/N$.
29. Seja $G$ um grupo de ordem $|G| = 2p$ onde $p$ é um primo ímpar. Prove que: ou $G$ é cíclico ou $G \simeq D_p$ o grupo dihedral de ordem $2p$.
30. Seja $G$ um grupo de ordem 12 tal que $G \not\simeq A_4$ ($G$ não é isomorfo ao grupo $A_4$). Então prove que $\exists\, y \in G$ tal que $\mathcal{O}(y) = 6$.
31. Seja $G$ um p-grupo não abeliano de ordem $|G| = p^3$. Prove que $Z(G) = G'$ é um subgrupo de ordem $p$.
32. Seja $P$ um p-sylow subgrupo de um grupo finito $G$ e seja $H$ um subgrupo normal de $G$. Então, se $P \trianglelefteq H$ temos $P \trianglelefteq G$.
33. Se $G$ é um grupo cíclico infinito então $G$ é isomorfo ao grupo aditivo dos inteiros.
34. Seja $G$ um grupo cíclico finito de ordem $n$. Prove que se $d$ é um divisor de $n$ então existe um único subgrupo $H$ de $G$ de ordem $d$. Em particular,
    Todo subgrupo $H$ de um grupo cíclico $G$ é característico em $G$.
35. Seja $T$ um subgrupo cíclico normal em $G$. Prove que: se $U \leq T$ então $U \trianglelefteq G$.
36. Seja $G$ um grupo abeliano finito de ordem $|G| = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$ onde $p_1, \dots, p_r$ são os distintos primos divisores de $|G|$ e $\alpha_1, \dots, \alpha_r \in \mathbb{N} - \{0\}$. Prove que:
    a) $G_{p_i} = \{x \in G : x^{p_i^m} = e$ para algum inteiro $m \geq 0\}$ é um subgrupo de $G$.
    b) se $g \in G\ \exists$ únicos $g_i \in G_{p_i}$, $i = 1, \dots, r$ tais que: $g = g_1 \cdot g_2 \dots g_r$.

c) $G \simeq G_{p_1} \times G_{p_2} \times \ldots \times G_{p_r}$
d) $|G_{p_i}| = p_i^{\alpha_i}$ e $G_{p_i}$ é o único $p_i$-sylow subgrupo de $G$.

37. Se $N \trianglelefteq G$ e $N \leq H \leq G$ então $\dfrac{G/N}{H/N} \simeq G/H$.

38. Se $G = \mathbb{Z}_p, +$, $p$ primo então Aut $G$ é um grupo cíclico de ordem igual a $p - 1$.

## §5 A simplicidade dos grupos $A_n$, $n \geq 5$

Nesse parágrafo apresentaremos a noção de solubilidade e provaremos a simplicidade dos grupos $A_n$, $n \geq 5$. Em particular teremos a não solubilidade dos grupos $S_n$, $n \geq 5$.

Um grupo $G$ diz-se *solúvel* se existem subgrupos $\{e\} = G_0 \leq G_1 \leq \leq G_2 \leq \ldots \leq G_{n-1} \leq G_n = G$ tais que:

(1) $G_{i-1} \trianglelefteq G_i \; \forall i \in \{1, 2, \ldots, n\}$
(2) $G_i/G_{i-1}$ é abeliano $\forall i \in \{1, 2, \ldots, n\}$.

Assim, grupos abelianos e $p$-grupos são exemplos de grupos solúveis. Os grupos $S_3$, $A_4$ e $S_4$ são também exemplos de grupos solúveis embora não sejam nem abelianos nem que se $H$ é um desses 3 grupos acima então $Z(H) = \{e\}$.

PROPOSIÇÃO 12. a) *Todo subgrupo de um grupo solúvel é solúvel.*
b) *Todo quociente de um grupo solúvel é solúvel.*
c) *Seja $G$ um grupo e $N \trianglelefteq G$. Então, $G/N$ solúvel e $N$ solúvel $\Rightarrow G$ solúvel.*

*Demonstração.*

a) Seja $G$ um grupo solúvel e $\{e\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq \leq G_{n-1} \leq G_n = G$ uma "cadeia solúvel" de $G$, isto é,

(1) $G_{i-1} \trianglelefteq G_i \;\; \forall i \in \{1, 2, \ldots, n\}$

e

(2) $G_i/G_{i-1}$ abeliano $\forall i \in \{1, 2, \ldots, n\}$.

Seja $L$ um subgrupo qualquer de $G$ e defina $L_i = L \cap G_i$ $\forall i \in \{0, 1, \ldots, n\}$. Claramente temos $L_0 = \{e\} \leq L_1 \leq \ldots \leq L_{n-1} \leq \leq L_n = L \cap G = L$.

Primeiramente vamos provar que $L_{i-1} \trianglelefteq L_i \;\; \forall i \in \{1, 2, \ldots, n\}$.

De fato, se $x \in L_{i-1} = G_{i-1} \cap L$ e $g \in L_i = G_i \cap L$ então $x \in G_{i-1}$ e $x \in L, g \in G_i$ e $g \in L$. Assim, $x^g = g^{-1} \cdot x \cdot g \in L$ e como $G_{i-1} \trianglelefteq G_i$ também temos $x^g = g^{-1} \cdot x \cdot g \in G_{i-1}$, ou seja, $x^g \in L_{i-1} = G_{i-1} \cap L$.

Agora para provarmos que $L_i/L_{i-1}$ é abeliano basta observar que:

$$\psi_i : L_i \to G_i/G_{i-1}$$
$$x \rightsquigarrow \psi_i(x) = G_{i-1} \cdot x$$

é um homomorfismo cujo núcleo é exatamente

$$N(\psi_i) = \{x \in L_i : x \in G_{i-1}\} = L_{i-1}.$$

Assim pelo 1.º Teorema de homomorfismo teremos:

$$L_i/L_{i-1} \simeq \operatorname{Im} \psi_i \leq G_i/G_{i-1}$$

e como $G_i/G_{i-1}$ é abeliano segue imediatamente que $L_i/L_{i-1}$ é também abeliano $\forall\, i \in \{1, 2, \ldots, n\}$ e isto demonstra o item a).

b) Seja $N \trianglelefteq G, \pi : G \to \bar{G} = G/N$ a projeção canônica. Suponhamos $G$ solúvel. Vamos provar que $\pi(G) = \bar{G}$ é também solúvel.

Seja $\{e\} = G_0 \leq G_1 \leq \ldots \leq G_{i-1} \leq G_i \leq \ldots \leq G_{n-1} \leq G_n = G$ tal que:

(1) $G_{i-1} \trianglelefteq G_i \;\forall\, i \in \{1, 2, \ldots, n\}$
(2) $G_i/G_{i-1}$ abelianos $\forall\, i \in \{1, 2, \ldots, n\}$.

Se $\bar{G}_i = \pi(G_i) = \{\bar{g}_i = \pi(g_i) : g_i \in G_i\}$ então temos que:

$$\{\bar{e}\} = \bar{G}_0 \leq \bar{G}_1 \leq \ldots \leq \bar{G}_{i-1} \leq \bar{G}_i \leq \ldots \leq \bar{G}_{n-1} \leq \bar{G}_n = \bar{G}$$

Vamos provar que:

(1) $\bar{G}_{i-1} \trianglelefteq \bar{G}_i \;\forall\, i \in \{1, 2, \ldots, n\}$
(2) $\bar{G}_i/\bar{G}_{i-1}$ abeliano $\forall\, i \in \{1, 2, \ldots, n\}$.

De fato, seja $i \in \{1, 2, \ldots, n\}$.

(1) se $\pi_i = \pi|_{G_i} : G_i \to \bar{G}_i$ é o homomorfismo restrição (é sobrejetivo) temos pelo teorema da correspondência que: $G_{i-1} \trianglelefteq G_i \Rightarrow \Rightarrow \pi_i(G_{i-1}) \trianglelefteq \bar{G}_i$ e isto demonstra (1) pois $\pi_i(G_{i-1}) = \pi(G_{i-1}) = \bar{G}_{i-1}$.

(2) sejam $u, v \in \bar{G}_i/\bar{G}_{i-1} = \pi(G_i)/\pi(G_{i-1})$. Vamos provar que $u.v = = v.u$ e isto nos diz que $\bar{G}_i/\bar{G}_{i-1}$ é abeliano.

De fato,

$$u = \pi(G_{i-1}) \cdot \pi(g_i) \text{ para algum } \pi(g_i) \in \pi(G_i),\; g_i \in G_i.$$
$$v = \pi(G_{i-1}) \cdot \pi(h_i) \text{ para algum } \pi(h_i) \in \pi(G_i),\; h_i \in G_i.$$

Observe que $G_i/G_{i-1}$ é abeliano e assim temos que:

$$(G_{i-1} \cdot g_i) \cdot (G_{i-1} \cdot h_i) = (G_{i-1} \cdot h_i)(G_{i-1} \cdot g_i)$$

ou seja, $$G_{i-1} \cdot g_i \cdot h_i = G_{i-1} \cdot h_i \cdot g_i.$$

Daí segue imediatamente que:

$$\exists\, x_{i-1} \in G_{i-1} \text{ tal que: } g_i \cdot h_i = x_{i-1}(h_i \cdot g_i).$$

Agora,

$$u.v = \pi(G_{i-1}) \cdot \pi(g_i) \cdot \pi(h_i) = \pi(G_{i-1}) \cdot (g_i \cdot h_i) =$$
$$= \pi(G_{i-1}) \cdot \pi(x_{i-1}) \cdot \pi(h_i \cdot g_i)$$

ora como $\pi(x_{i-1}) \in \pi(G_{i-1})$ temos que:

$$u.v = \pi(G_{i-1}) \cdot \pi(h_i) \cdot \pi(g_i) = v.u$$

e isto demonstra o item *b*).

c) Seja $G$ um grupo, $N \trianglelefteq G$ e seja $\pi : G \to G/N = \bar{G}$ a projeção canônica.

Suponhamos que $\bar{G} = G/N$ e $N$ sejam solúveis.
Assim existem (pelo teorema da correspondência) subgrupos

$$N = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{n-1} \subseteq G_n = G$$

tais que:

(1) $\bar{G}_{i-1} = G_{i-1}/N \trianglelefteq G_i/N \ \ \forall\, i \in \{1, 2, \ldots, n\}$

(2) $\bar{G}_i/\bar{G}_{i-1}$ abeliano $\forall\, i \in \{1, 2, \ldots, n\}$.

Ainda pelo teorema da correspondência temos que:

(1)′ $G_{i-1} \trianglelefteq G_i \ \ \forall\, i \in \{1, 2, \ldots, n\}$,

e por um exercício do parágrafo anterior temos também que:

(2)′ $G_i/G_{i-1} \simeq \dfrac{G_i/N}{G_{i-1}/N} = \bar{G}_i/\bar{G}_{i-1}$ abeliano $\forall\, i \in \{1, 2, \ldots, n\}$.

Mais ainda como $N$ é solúvel segue que:

$$\exists\, \{e\} = N_0 \leq N_1 \leq \ldots \leq N_{r-1} \leq N_r = N$$

tais que:

(1)″ $N_{j-1} \trianglelefteq N_j \ \ \forall\, j \in \{1, 2, \ldots, r\}$

(2)″ $N_j/N_{j-1}$ abeliano $\forall\, j \in \{1, 2, \ldots, r\}$

Portanto existem subgrupos $N_0, \ldots, N_r, G_0, \ldots G_n$ tais que:

$$\{e\} = N_0 \leq N_1 \leq \ldots \leq N_{r-1} \leq N_r \leq N =$$
$$= G_0 \leq G_1 \leq \ldots \leq G_{n-1} \leq G_n = G$$

nas condições (1)', (2)' e (1)'' e (2)'', ou seja, $G$ é solúvel. ■

Na classe dos grupos solúveis estão os grupos abelianos, os p-grupos e entre outros grupos $S_3$, $A_4$ e $S_4$. Como o produto direto de grupos solúveis é ainda solúvel podemos, a partir de todos esses grupos, montar infinitos outros exemplos de grupos solúveis. Enunciaremos agora dois resultados famosos na Teoria dos grupos finitos, o primeiro provado por W. Burnside no início do século e o segundo, no início da década de 1960, por W-Feit, e J. Thompson.

No início do século o matemático W. Burnside provou, usando a técnica de representar o grupo por grupos de matrizes, o seguinte teorema:

TEOREMA 8 $p^a \cdot q^b$ (Burnside). *Todo grupo finito cuja ordem é divisível no máximo por dois primos é solúvel.*

Burnside também conjecturou algo que parecia tarefa impossível de ser vencida em nosso século.

Conjectura de Burnside:

Todo grupo de ordem impar é solúvel.

Os matemáticos W. Feit e J. Thompson, no trabalho mais celebrado da Teoria dos grupos finitos, responderam na afirmativa tal conjectura num trabalho de mais de 200 páginas publicado no Pacific Journal of Mathematics em 1963.

TEOREMA 9 (W. Feit & J. Thompson). *Todo grupo de ordem impar é solúvel.*

Antes de provarmos a simplicidade dos grupos $A_n$, $n \geq 5$, precisamos desenvolver algumas definições e proposições sobre permutações.

Dizemos que uma permutação $\sigma \in S_n$ é um *r-ciclo* de $S_n$ $r \geq 2$ se $\exists\, i_1, i_2, \ldots, i_r$ distintos elementos de $\{1, 2, \ldots, n\}$ tais que:

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$$

e

$$\sigma(j) = j \ \forall j \in \{1, 2, \ldots, n\} - \{i_1, i_2, \ldots, i_r\}.$$

Nesse caso usaremos a notação $\sigma = (i_1, i_2, \ldots, i_r) \in S_n$ em vez da notação anterior de permutação. Observem que usando essa notação de ciclos

temos que especificar os grupos $S_n$ a que elas pertencem. Por exemplo, os ciclos (123) se considerados como elementos de $S_4$ fixam apenas o simbolo 4 enquanto que considerados em $S_5$ fixam os símbolos 4 e 5. Observem também que um r-ciclo de $S_n$ pertence ao grupo $A_n \Leftrightarrow r$ é ímpar. Sejam $\sigma = (i_1\, i_2 \ldots i_r)$ e $\tau = (j_1\, j_2 \ldots j_s)$ dois ciclos de $S_n$. Dizemos que $\sigma$ e $\tau$ são dois ciclos *disjuntos* se $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\} = \emptyset$.

Observe que se $\sigma$ e $\tau$ são dois ciclos disjuntos de $S_n$ então como permutações de $S_n$ eles comutam entre si, isto é, $\sigma \circ \tau = \tau \circ \sigma$. Para ver isto basta observar que os simbolos do conjunto $\{1, 2, \ldots, n\}$ que são movidos por $\sigma$ são necessariamente fixados por $\tau$ e vice-versa.

Por exemplo, os elementos do grupo $S_3$ são: e, (12), (13), (23), (123) e (132) e os elementos do grupo $A_4$ são: e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (2,3,4) e (243). Aqui o elemento (12)(34) representa a seguinte permutação $\sigma \in S_4$ produto dos dois 2-ciclos (12) e (34) de $S_4$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$

Observe também que (12) representa a permutação de $S_4$ fixando os símbolos 3 e 4 e movendo os símbolos 1 e 2, enquanto que (34) representa a permutação de $S_4$ fixando os símbolos 1 e 2 e movendo os símbolos 3 e 4. Ambos os 2-ciclos (12) e (34) são permutações ímpares porém $\sigma = (12)(34)$ é uma permutação par como produto de duas permutações ímpares.

Provaremos agora um teorema relativo a essa idéia de representar uma permutação como produto de ciclos.

**TEOREMA 10.** *Toda permutação $e \neq \sigma \in S_n$ pode ser escrita de modo único (à menos da ordem) como produto de ciclos disjuntos.*

*Demonstração.* Antes de iniciarmos a demonstração do teorema acima observe que:

O único elemento de $S_1$ é a identidade e; os únicos elementos de $S_2$ são e e (12); os 6 elementos de $S_3$ são e, (12), (13), (23), (123) e (132); e finalmente os 24 elementos de $S_4$ são: e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243), (12), (13), (14), (23), (24), (34), (1234), (1432), (1324), (1423), (1243) e (1342).

Seja $\sigma \in S_n$, $\sigma \neq e$. Vamos a seguir definir a seguinte relação entre pares de elementos do conjunto $\{1, 2, 3, \ldots, n\}$. Se $x, y \in \{1, 2, 3, \ldots, n\}$, $x \underset{\sigma}{\sim} y \Leftrightarrow \exists\, m \in \mathbb{Z}$ tal que $y = \sigma^m(x)$.

Afirmamos que $\underset{\sigma}{\sim}$ define uma relação de equivalência no conjunto $\{1, 2, 3, \ldots, n\}$.

De fato, se $x, y, z \in \{1, 2, 3, \ldots, n\}$

(i) $x \underset{\sigma}{\sim} x$ pois $x = \sigma^0(x)$

(ii) $x \underset{\sigma}{\sim} y \Rightarrow y \underset{\sigma}{\sim} x$ pois $y = \sigma^m(x) \Rightarrow x = \sigma^{-m}(y)$

(iii) $x \underset{\sigma}{\sim} y$, $y \underset{\sigma}{\sim} z \Rightarrow x \underset{\sigma}{\sim} z$ pois $y = \sigma^m(x)$, $z = \sigma^n(y) \Rightarrow z = \sigma^{m+n}(x)$.

Assim $\underset{\sigma}{\sim}$ determina uma partição no conjunto $\{1, 2, \ldots, n\}$ através do conjunto quociente.

Sejam $\bar{i}_1 = \{x \in \{1, 2, \ldots, n\} : x \underset{\sigma}{\sim} i_i\}, \ldots,$ $\bar{j}_1 = \{x \in \{1, 2, \ldots, n\} : x \underset{\sigma}{\sim} j_1\}, \ldots, \bar{\ell}_1 = \{x \in \{1, 2, \ldots, n\} : x \underset{\sigma}{\sim} \ell_1\}$ as distintas classes de equivalência relativamente a $\underset{\sigma}{\sim}$ (com representantes $i_1, \ldots, j_1, \ldots, \ell_1$) contendo mais de um elemento.

Assim $|\bar{i}_1| > 1, \ldots, |\bar{j}_1| > 1, \ldots, |\bar{\ell}_1| > 1$ (existem tais classes pois $\sigma \neq e$).

Se $Z$ é o subconjunto de $\{1, 2, \ldots, n\}$ tal que $\sigma(z) = z$ $\forall z \in Z$, então temos que:

$$\{1, 2, \ldots, n\} = Z \cup \bar{i}_1 \cup \ldots \cup \bar{j}_1 \cup \ldots \cup \bar{\ell}_1 \text{ (união disjunta)}$$

Se $H = \langle \sigma \rangle = \{\sigma^m : m \in Z\} \leq S_n$ então a relação de equivalência $\underset{\sigma}{\sim}$ poderia também ser definida por,

$$x \underset{\sigma}{\sim} y \Leftrightarrow \exists\, h \in H \text{ tal que } y = h(x).$$

Como $S_n$ é um grupo finito temos que $|H| = k < \infty$ e mais ainda $H = \langle \sigma \rangle = \{e, \sigma, \sigma^2, \ldots, \sigma^{k-1}\}$.

Portanto nossa relação de equivalência poderia ainda ser definida por:

$$x \underset{\sigma}{\sim} y \Leftrightarrow \exists\, m,\ 0 \leq m \leq k - 1 \text{ tal que } y = \sigma^m(x).$$

Assim, $\sigma^k(i_1) = i_1, \ldots, \sigma^k(j_1) = j_1, \ldots,$ $\sigma^k(\ell_1) = \ell_1$. Vamos definir os seguintes números:

Seja $r$ o menor inteiro, $1 \leq r \leq k$, tal que $\sigma^r(i_1) = i_1$; etc, etc, .... Seja $s$ o menor inteiro, $1 \leq s \leq k$ tal que $\sigma^s(j_1) = j_1$, etc, etc, .... Seja $t$ o menor inteiro $1 \leq t \leq k$ tal que $\sigma^t(\ell_1) = \ell_1$.

Ora, como $\bar{i}_1 = \{i_1, \sigma(i_1), \sigma^2(i_1), \ldots\}$, etc, $\ldots, \bar{j}_1 = \{j_1, \sigma(j_1), \sigma^2(j_1), \ldots\}$, etc, etc, $\ldots, \bar{\ell}_1 = \{\ell_1, \sigma(\ell_1), \sigma^2(\ell_1), \ldots\}$ segue imediatamente que:

$$\bar{i}_1 = \{i_1, \sigma(i_1), \sigma^2(i_1), \ldots, \sigma^{r-1}(i_1)\}, \text{ etc, etc } \ldots,$$
$$\bar{j}_1 = \{j_1, \sigma(j_1), \sigma^2(j_1), \ldots, \sigma^{s-1}(j_1)\}, \text{ etc, etc } \ldots,$$
$$\bar{\ell}_1 = \{\ell_1, \sigma(\ell_1), \sigma^2(\ell_1), \ldots, \sigma^{t-1}(\ell_1)\}$$

são as classes contendo mais de um elemento.

Definindo $\sigma^m(i_1) = i_{m+1}$, $\sigma^p(j_1) = j_{p+1}$, $\sigma^q(\ell_1) = \ell_{q+1}$ onde $0 \leq m \leq r-1$, $0 \leq p \leq s-1$ e $0 \leq q \leq t-1$ nós temos que:

$$\bar{i}_1 = \{i_1, i_2, i_3, \ldots, i_r\}, \text{ etc, etc, } \ldots, \bar{j}_1 = \{j_1, j_2, j_3, \ldots, j_s\},$$

etc, etc, $\ldots, \bar{\ell}_1 = \{\ell_1, \ell_2, \ell_3, \ldots, \ell_t\}$ são as classes contendo mais de um elemento e mais ainda:

$\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \ldots$, $\sigma(i_{r-1}) = i_r$, $\sigma(i_r) = i_1$, etc, etc, $\ldots$, $\sigma(j_1) = j_2$, $\sigma(j_2) = j_3, \ldots, \sigma(j_{s-1}) = j_s$, $\sigma(j_s) = j_1$, etc, etc, $\ldots$, $\sigma(\ell_1) = \ell_2$, $\sigma(\ell_2) = \ell_3, \ldots$, $\sigma(\ell_{t-1}) = \ell_t$, $\sigma(\ell_t) = \ell_1$.

Afirmamos agora que:

$$(*)\ \sigma = (i_1\, i_2\, i_3 \ldots i_r) \ldots (j_1\, j_2\, j_3 \ldots j_s) \ldots (\ell_1\, \ell_2\, \ell_3 \ldots \ell_s)$$

De fato, $G = Z \cup \{i_1, i_2, \ldots, i_r\} \cup \ldots \cup \{j_1, j_2, \ldots, j_s\} \cup \ldots \cup \{\ell_1, \ell_2, \ldots, \ell_t\}$.

Se $x \in \mathbb{Z}$ ambos os membros da igualdade $(*)$ fixam o elemento $x \in \{1, 2, \ldots, n\}$.

Se $x \notin Z$ então $x$ está em alguma classe, digamos $\bar{j}_1$, assim $x \in \{j_1, j_2, \ldots, j_s\}$. Se $\sigma_{j_1} = (j_1\, j_2 \ldots j_s)$ é o ciclo definido pela classe $\bar{j}_1$, então claramente temos que: $\sigma|_{\bar{j}_1} = \sigma_{j_1}$ e portanto a igualdade $(*)$ se verifica quando aplicada ao elemento $x \in \{1, 2, \ldots, n\}$. Assim fica provada a primeira parte do teorema com a validade da igualdade $(*)$.

Deixamos como exercício a prova da unicidade da decomposição (a menos da ordem dos ciclos). ∎

Se $\sigma$ e $\tau$ são duas permutações em $S_n$ tais que:

$$\sigma = (i_1 \ldots i_r) \ldots (j_1 \ldots j_s) \ldots (\ell_1 \ldots \ell_s) \quad \text{e}$$
$$\tau = (i'_1 \ldots i'_r) \ldots (j'_1 \ldots j_s) \ldots (\ell'_1 \ldots \ell'_s)$$

e dizemos que $\sigma$ e $\tau$ possuem a *mesma estrutura de ciclos.*

**PROPOSIÇÃO 13.** *Sejam $\sigma$ e $\tau \in S_n$. Então, $\sigma$ e $\tau$ são conjugados em $S_n \Leftrightarrow \sigma$ e $\tau$ possuem a mesma estrutura de ciclos.*

*Demonstração.*

$(\Rightarrow)$: Seja $f \in S_n$ tal que $\tau = \sigma^f = f^{-1} \circ \sigma \circ f$ e seja

$$\sigma = (i_1\, i_2 \ldots i_r) \ldots (j_1\, j_2 \ldots j_s) \ldots (\ell_1\, \ell_2 \ldots \ell_t)$$

então é suficiente provarmos que:

$$\sigma^f = (f^{-1}(i_1)f^{-1}(i_2)\dots f^{-1}(i_r))\dots(f^{-1}(j_1)f^{-1}(j_2)\dots f^{-1}(j_s))\dots$$
$$\dots(f^{-1}(\ell_1)f^{-1}(\ell_2)\dots f^{-1}(\ell_t)).$$

De fato,

se $\sigma(x) = y$ então $\sigma^f(f^{-1}(x)) = (f^{-1}\circ\sigma)(f(f^{-1}(x))) = f^{-1}(\sigma(x)) = f^{-1}(y)$.

($\Leftarrow$): Sejam $\sigma = (i_1\, i_2 \dots i_r)\dots(j_1 j_2 \dots j_s)\dots(\ell_1\, \ell_2 \dots \ell_s)$ e $\tau = (i'_1\, i'_2 \dots i'_r)\dots$ $\dots(j'_1 j'_2 \dots j'_s)\dots(\ell'_1\, \ell'_2 \dots \ell'_s)$ são duas permutações de $S_n$ com mesma estrutura de ciclos então segue imediatamente que: $\tau = \sigma^g$ onde $g \in S_n$ definida por:

$$\begin{array}{lll} g(i'_k) = i_k & 1 \le k \le r\,, & \text{etc, etc, ...} \\ g(j'_m) = j_m & 1 \le m \le s\,, & \text{etc, etc, ...} \\ g(\ell'_q) = \ell_q & 1 \le q \le t. & \end{array}$$

e $g$ (arbitrariamente) definido nos restantes simbolos não envolvidos na definição acima. ■

Observe que (123) e (132) não são conjugados em $A_4$ mas pela proposição anterior são conjugadas em $S_4$. Daremos o nome de *transposição em $S_n$* a qualquer 2-ciclo $(ij)$ do grupo $S_n$.

PROPOSIÇÃO 14. a) *O grupo $S_n$, $n \ge 2$ é gerado pelo conjunto de todas as transposições de $S_n$.*

b) *$\sigma \in S_n$, $n \ge 3$ é par $\Leftrightarrow$ $\sigma$ é um produto de um número par de transposições.*

c) *O grupo $A_n$, $n \ge 3$, é gerado pelo conjunto de todos os 3-ciclos de $S_n$.*

*Demonstração.* a) Pelo Teorema 11 é suficiente provarmos que um r-ciclo $(i_1\, i_2 \dots i_r)$, $r \ge 3$, é produto de transposições e isto segue imediatamente da igualdade:

$$(i_1\, i_2 \dots i_r) = (i_1\, i_r)(i_1\, i_{r-1})\dots(i_1 i_2)$$

b) ($\Leftarrow$): se $\sigma = \tau_1 \cdot \tau_2 \dots \tau_{2k} \in S_n$ temos que se

$$P = P(x_1, \dots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j) \text{ então, } P^\sigma = (-1)^{2k} \cdot P = P$$

e portanto $\sigma \in A_n$.

($\Rightarrow$): Seja $\sigma \in A_n$. Pelo Teorema 11 podemos escrever:

$$\sigma = (i_1\, i_2 \dots i_r)\dots(j_1 j_2 \dots j_s)\dots(\ell_1\, \ell_2 \dots \ell_t)$$

Ora sabemos que:

$(i_1\, i_2 \dots i_r)$ é ímpar $\Leftrightarrow$ $r$ é par $\Leftrightarrow$ $(r-1)$ é ímpar e mais ainda: $(i_1\, i_2 \dots i_r) = (i_1\, i_r)(i_1 i_{r-1}) \dots (i_1\, i_2)$, ou seja, $(i_1\, i_2 \dots i_r)$ é um produto de $(r-1)$ transposições.

Como em uma permutação par o número de ciclos não pertencentes a $A_n$ deve aparecer um número par de vezes o item b) segue.

c) Pelo item b) é bastante observar que:

$$(ab)(cd) = (bdc)(acb)$$

$$(ab)(ac) = (acb)$$

e isto demonstra a Proposição 14. ■

**COROLÁRIO 1.** *Os ciclos* (12) *e* (1 2 ... *n*) *geram o grupo* $S_n$.

*Demonstração.* Seja $t = (12)$ e $a = (1\,2 \dots n)$, e seja $G = \langle a, t \rangle$ o grupo gerado por $a$ e $t$.

Assim, $a^{-1}ta = (23)$, $a^{-2}ta^2 = (34)$, etc, etc, ... $(m, m+1)$ estão em $G$.

Portanto, $G$ contém as transposições:

$$(12)(23)(12) = (13),\ (13)(34)(13) = (14),\ \text{etc}, \dots (1m)$$

Daí segue que: $\forall\, m, r \in \{1, 2, \dots, n\}$, $m \neq r$ $(1m)(1r)(1m) = (mr) \in G$ e pela proposição anterior tem-se $G = S_n$. ■

**PROPOSIÇÃO 15.** *Sejam* $a, b \in \{1, 2, \dots, n\}$, $a \neq b$ *fixos. Então, o grupo* $A_n$, $n \geq 3$, *é gerado pelo conjunto de todos os 3-ciclos de* $S_n$ *do tipo* $(abk)$, *onde* $1 \leq k \leq n$, $k \neq a$, $k \neq b$.

*Demonstração.* Sabemos que $A_n$ é gerado por todos os 3-ciclos $(efg)$ de $S_n$. Agora, $(efg) = (agf)(aef)(aeg)$ e assim é suficiente provarmos que os 3-ciclos do tipo $(afg)$ podem ser escritos como produto de 3-ciclos do tipo $(abk)$, $1 \leq k \leq n$, $k \neq a$, $k \neq b$.

Assim, se $f = b$ nada temos à demonstrar, e se $g = b$ também temos $(afg) = (afb) = (abf)^2 = (abf)(abf)$ e também nada temos a demonstrar. Suponhamos agora que: $f \neq b$ e $g \neq b$. Nesse caso basta observar que:

$$(afg) = (abg)(abg)(abf)(abg)$$

e isto demonstra a Proposição 15. ■

TEOREMA 11. *O grupo $A_n$, $n \geq 5$, simples.*

COROLÁRIO 1. *O grupo $S_n$, $n \geq 5$, não é solúvel.*

*Demonstração do corolário.* Basta observar que $A_n \leq S_n$ e $A_n$ é não solúvel.

*Demonstração do Teorema* 12. Seja $\{e\} \neq N \trianglelefteq A_n$. Vamos provar $N = A_n$.

*Caso* 1: $N$ contém um 3-ciclo $(abc)$.

Assim $N$ contém $(bac) = (abc)^2$. Agora se $\sigma = (ab)(ck) \in A_n$ e $N \leq A_n$ temos que:

$$(abk) = \sigma^{-1}(bac)\sigma \in N \qquad \begin{matrix} \forall\, k \in \{1, 2, \ldots, n\} \\ k \neq a,\ k \neq b \end{matrix}$$

Pela Proposição 14 então $N = A_n$.

Agora para completar a demonstração vamos produzir um 3-ciclo $(abc) \in N$.

Como $N \neq \{e\}$ podemos escolher $\tau \in N$, $\tau \neq e$, fixando o número máximo possível de símbolos. Vamos provar que $\tau$ é uma 3-ciclo.

Suponhamos por absurdo que $\tau$ não é um 3-ciclo. Assim pelo menos 4 símbolos aparece na representação de $\tau$ como produto de ciclos. Portanto temos duas possibilidades

(1) $\tau = (abcdf \ldots) \ldots$ (já que $(abcd) \notin A_n$)

ou

(2) $\tau = (ab)(cd) \ldots$

Agora seja $\sigma = (cde) \in A_n$. Então teremos,

(1) $\tau_1 = \sigma \cdot \tau \cdot \sigma^{-1} = (cdf)(abcdf \ldots) \ldots (ced) = \tau_1 = (abdfc \ldots) \ldots \in N$

(2) $\tau_1 = \sigma \cdot \tau \cdot \sigma^{-1} = (ab)(df) \ldots \in N$

Em ambos os casos $\tau \neq \tau_1$. Agora consideramos $\gamma = \tau^{-1} \cdot \tau_1 \in N$. Como $\tau \neq \tau_1$ segue que $\gamma \neq e \in S_n$ e mais ainda verifica-se que $\gamma = \tau^{-1} \cdot \tau_1$ fixa mais elementos do que $\tau$ o que é uma contradição.

Portanto $\tau = (abc)$ é um 3-ciclo em $N$ e pelo caso 1 $N = A_n$ demonstrando o Teorema 12. ■

EXERCÍCIOS

1. Seja $G$ um grupo. Defina, $G^{(0)} = G$, $G^{(1)} = [G, G] = 0$ grupo gerado por todos os elementos $[x, y] = x^{-1}y^{-1}xy$ (chamado *o grupo comutador de G*), $G^{(2)} = [G^{(1)}, G^{(1)}]$, … $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$, $n \geq 1$.

Prove que:
$G$ é solúvel $\Leftrightarrow \exists\, n$ inteiro $\geq 1$ tal que $G^{(n)} = \{e\}$.

2. Prove que se $G$ é solúvel $\exists\, \{e\} \neq M \trianglelefteq G$, $M$ abeliano.
3. Prove que os seguintes grupos são solúveis: $S_3$, $A_4$, $D_n$, $n \geq 3$, $S_4$.
4. Prove que se $G$ é um grupo tal que Aut $G$ é solúvel então $G$ é também solúvel
5. Sejam $H$ e $K$ subgrupos solúveis de um grupo $G$. Prove que: se $K \leq G$ então $HK$ é também um subgrupo solúvel de $G$.
6. Prove que se $n \geq 5$ então $A_n$ é o único subgrupo normal de $S_n$ diferente de $\{e\}$ e $S_n$.
7. Prove que $S_n$ é isomorfo a um subgrupo do grupo $A_{n+2}$.
8. Seja $S = \{1, 2, \ldots, n, \ldots\}$ e seja $(abc)$ um 3-ciclo no grupo $\mathscr{P}(S)$ das permutações de $S$, (isto é, $(abc)$ fixa $j$ $\forall\, j \in S - \{a, b, c\}$).

   Defina $A_\infty$ como o subgrupo de $\mathscr{P}(S)$ gerado por todos os 3-ciclos $(abc) \in \mathscr{P}(S)$.

   Pergunta-se:

   (a) É $A_\infty$ um grupo simples?

   (b) Se $G$ é um grupo finito simples então $G$ é isomorfo a um subgrupo de $A_\infty$

   (*Sugestão*: Usar o Teorema de Cayley e o Exercício 7).

# TEORIA DE GALOIS ELEMENTAR

Nesse capítulo provaremos o teorema fundamental de Galois para extensões $L \supset K$ finitas tais que $\mathbb{C} \supset L \supset K \supset \mathbb{Q}$. Exibiremos também um polinômio de grau 5, com coeficientes inteiros, que não é solúvel por meio de radicais. Todas extensões $L \supset K$ aqui consideradas são subcorpos de $\mathbb{C}$ contendo $\mathbb{Q}$.

## §1 Extensões galoisianas e extensões normais

Dizemos que uma extensão finita $L \supset K$ é uma *extensão galoisiana* se $\exists f(x) \in K[x]$ tal que $L = \mathrm{Gal}(f, K)$, e dizemos que uma extensão algébrica $L \supset K$ é *normal* se $\forall g(x) \in K[x]$, irredutível sobre $K$ que possui uma raiz $\alpha \in L$ possui todas as suas raízes complexas em $L$.

Observe que se $L \supset M \supset K$ são extensões tais que $L \supset K$ é galoisiana então $L \supset M$ é também galoisiana, porém $M \supset K$ não é necessariamente galoisiana como mostra o exemplo $L = \mathrm{Gal}(x^3 - 2, \mathbb{Q})$, $M = \mathbb{Q}[\sqrt[3]{2}]$ e $K = \mathbb{Q}$.

Vamos mostrar nesse parágrafo que uma extensão finita $L \supset K$ é galoisiana se e somente se $L \supset K$ é normal. Mas antes vamos dar algumas definições e provar alguns resultados sobre extensões de isomorfismos.

Sejam $K, K' \supset \mathbb{Q}$ corpos e $\sigma\colon K \to K'$, $a \mapsto a'$ um isomorfismo de $K$ sobre $K'$. Se $f(x) = a_0 + a_1x + \ldots + a_nx^n$ é um polinômio em $K[x]$ definimos $f^\sigma(x) = a'_0 + a'_1x + \ldots + a'_nx^n \in K'[x]$ onde $a'_i = \sigma(a_i)$; $i = 0, 1, \ldots, n$.

Observe que se $f(x) = f_1(x) \cdot f_2(x) \ldots f_k(x)$ onde $f_j(x) \in K[x]$ são irredutíveis sobre $K, j = 1, \ldots, k$ então $f^\sigma(x) = f_1^\sigma(x) \cdot f_2^\sigma(x) \ldots f_k^\sigma(x)$ onde $f_j^\sigma(x) \in K'[x]$ são irredutíveis sobre $K', j = 1, \ldots, k$.

Em particular se todas as raízes de $f(x)$ estão em $K$ temos que cada $f_j(x)$ possui grau 1 e portanto cada $f_j^\sigma(x)$ também possui grau 1, e daí segue imediatamente que todas as raízes de $f^\sigma$ estão em $K'$.

**PROPOSIÇÃO 1.** *Sejam $K, K' \supset \mathbb{Q}$ corpos e $\sigma: K \to K'$ um isomorfismo, e $h(x) \in K[x]$ um polinômio irredutível sobre $K$.*

*Se $\alpha$ é uma raiz de $h(x)$ em $\mathbb{C}$ e $\beta$ é uma raiz de $h^{\sigma}(x)$ em $\mathbb{C}$, então existe um único isomorfismo $\hat{\sigma}: K[\alpha] \to K'[\beta]$ tal que $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma}|_K = \sigma$.*

*Demonstração.* Seja $\alpha$ uma raiz qualquer de $h(x) \in K[x]$ e $\beta$ uma raiz de $h^{\sigma}(x) \in K'[x]$. Sabemos do Capítulo 5 que $K[\alpha]$ e $K'[\beta]$ são corpos e mais ainda se grau $h(x)$ = grau $h^{\sigma}(x) = r$ segue que:

(1) $K[\alpha] = \{a_0 + a_1\alpha + \ldots + a_{r-1}\alpha^{r-1} : a_i \in K\}$ e $1, \alpha, \alpha^2, \ldots, \alpha^{r-1}$ é uma base do espaço vetorial $K[\alpha]$ sobre o corpo $K$.

(2) $K'[\beta] = \{a'_0 + a'_1\beta + \ldots + a'_{r-1}\beta^r : a'_i \in K'\}$ e $1, \beta, \beta^2, \ldots, \beta^{r-1}$ é uma base do espaço vetorial $K'[\beta]$ sobre o corpo $K'$.

Agora é fácil ver que $\hat{\sigma}: K[\alpha] \to K'[\beta]$ definido por $\sigma(a_0 + a_1\alpha + + \ldots + a_{r-1}\alpha^{r-1}) = \sigma(a_0) + \sigma(a_1)\beta + \ldots + \sigma(a_{r-1})\beta^{r-1}$ é um isomorfismo do corpo $K[\alpha]$ sobre o corpo $K'[\beta]$ tal que $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma}|_K = \sigma$, e claramente $\hat{\sigma}$ é o único com essas duas condições. ∎

**PROPOSIÇÃO 2.** *Sejam $K, K' \supseteq \mathbb{Q}$ corpos, $\sigma: K \to K'$ um isomorfismo, $f(x) \in K[x]$ e $\alpha$ uma raiz qualquer de $f(x)$ em $\mathbb{C}$. Então $\exists\ \beta$ raiz de $f^{\sigma}(x)$ em $\mathbb{C}$ e existe um isomorfismo*

$$\sigma_1: K[\alpha] \to K'[\beta]$$

*tal que:*

$$\sigma_1(\alpha) = \beta \text{ e } \sigma_1|_K = \sigma.$$

*Demonstração.* Seja $f(x) = f_1(x)^{m_1} \cdot f_2(x)^{m_2} \ldots f_k(x)^{m_k}$ onde $f_1(x), \ldots, f_k(x)$ são os distintos fatores irredutíveis de $f(x)$ em $K[x]$.

Assim $f^{\sigma}(x) = f_1^{\sigma}(x)^{m_1} \ldots f_k^{\sigma}(x)^{m_k}$ onde $f_1^{\sigma}(x), \ldots, f_k^{\sigma}(x)$ são os distintos fatores irredutíveis de $f^{\sigma}(x)$ em $K'[x]$.

Se $\alpha$ é raiz de $f(x)$ podemos assumir que $\alpha$ é raiz de $f_1(x)$ irredutível sobre $K$. Assim se $\beta$ é qualquer raiz do polinômio $f_1^{\sigma}(x)$ irredutíveis sobre $K'$ a Proposição 2 segue imediatamente da Proposição 1. ∎

**TEOREMA 1.** *Sejam $K, K' \supseteq \mathbb{Q}$ corpos, $\sigma: K \to K'$ um isomorfismo, $f(x) \in K[x]$ e $\alpha_1, \ldots, \alpha_r$ as distintas raízes de $f(x)$ em $\mathbb{C}$.*

*Se $L = Gal(f, K)$ e $L' = Gal(f^{\sigma}, K')$ então $\exists\ \hat{\sigma}: L \to L'$ um isomorfismo tal que $\hat{\sigma}|_K = \sigma$ e mais ainda $\hat{\sigma}(\alpha_1), \ldots, \hat{\sigma}(\alpha_r)$ são as distintas raízes de $f^{\sigma}(x)$ em $\mathbb{C}$.*

*Demonstração.* Se $f(x) \in K[x]$ possui uma única raiz $\alpha_1$ então temos $f(x) = (x - \alpha_1)^m$ em $\mathbb{C}[x]$, mas isto implica que $\alpha_1 \in K$ e portanto $\sigma(\alpha_1) \in K'$ é a única raiz de $f^{\sigma}(x)$ em $\mathbb{C}$ e teremos $L = K$, $L' = K'$ e $\hat{\sigma} = \sigma : L \to L'$.

Agora se $f(x) = f_1(x)^{m_1} \dots f_k(x)^{m_k}$ onde $f_i(x) \in K[x]$ são distintos polinômios irredutíveis sobre $K$ temos que $f^{\sigma}(x) = f_1^{\sigma}(x)^{m_1} \dots f_k^{\sigma}(x)^{m_k}$ onde $f_i^{\sigma}(x) \in K'[x]$ são distintos polinômios irredutíveis sobre $K'$.

Sabemos pela Proposição 2 do Capítulo 5 que o número $r$ de raízes distintos de $f(x)$ em $\mathbb{C}$ é igual a soma dos graus dos polinômios $f_1(x), \dots, f_k(x)$ e portanto temos como conseqüência que o número de raízes distintas de $f^{\sigma}(x)$ em $\mathbb{C}$ é também igual a $r$.

Sejam $\beta_1, \beta_2, \dots, \beta_r$ as $r$ distintas raízes em $\mathbb{C}$ do polinômio $f^{\sigma}(x) \in K'[x]$.

Seja $K_1 = K[\alpha_1], K_2 = K_1[\alpha_2], \dots, K_r = K_{r-1}[\alpha_r]$.

Assim temos que $L = K[\alpha_1, \dots, \alpha_r] = K_r$.

Pela proposição anterior $\exists\, \beta \in \{\beta_1, \dots, \beta_r\}$ e $\exists$ isomorfismo $\sigma$: $K[\alpha_1] \to K'[\beta]$ tal que $\sigma_1(\alpha_1) = \beta$ e $\sigma_1|_K = \sigma$. Chamando $\beta_1 = \sigma_1(\alpha_1) = \beta$ temos então que $\exists\, \beta_1 \in \{\beta_1, \dots, \beta_r\}$ e $\exists$ isomorfismo $\sigma_1 : K[\alpha_1] \to K'[\beta_1]$ tal que:

$$\sigma_1(\alpha_1) = \beta_1 \text{ e } \sigma_1|_K = \sigma.$$

Seja $K'[\beta_1] = K'_1$. Assim $\exists\, \sigma_1 : K_1 \to K'_1$ isomorfismo tal que $\sigma_1(\alpha_1) = \beta_1$ e $\sigma_1|_K = \sigma$.

Ora, como $f(x) \in K[x]$ e $\sigma_1|_K = \sigma$ segue imediatamente que $f(x) \in K_1[x]$ e $f^{\sigma_1}(x) = f^{\sigma}(x)$.

Aplicando novamente a Proposição 2 deste capítulo para os corpos $K_1, K'_1 \supseteq \mathbb{Q}$ e $\sigma_1 : K_1 \to K'_1$ chegamos que $\exists\, \beta \in \{\beta_1, \beta_2, \dots, \beta_k\}$ (o qual chamaremos de $\beta_2$) e $\exists\, \sigma_2 : K_1[\alpha_2] \to K'_1[\beta_2]$ isomorfismo tal que: $\sigma_2(\alpha_2) = \beta_2$ e $\sigma_2|_K = \sigma_1$. (Observe que $\sigma_2$ isomorfismo e $\alpha_1 \neq \alpha_2$ implica que $\beta_1 = \sigma_2(\alpha_1) \neq \sigma_2(\alpha_2) = \beta_2$).

Ora, como $\sigma_1|_K = \sigma$ segue imediatamente que,

$$\sigma_2|_K = \sigma \text{ e } \sigma_2(\alpha_1) = \beta_1, \ \sigma_2(\alpha_2) = \beta_2$$

e $\sigma_2$: $K[\alpha_1, \alpha_2] \to K'[\beta_1, \beta_2]$ é um isomorfismo.

Supondo que $\exists\, \sigma_{k-1} : K[\alpha_1, \dots, \alpha_{k-1}] \to K'[\beta_1, \dots, \beta_{k-1}]$ isomorfismo tal que: $\sigma_{k-1}(\alpha_i) = \beta_i, i = 1, 2, \dots, k-1$ e $\sigma_{k-1}|_K = \sigma$ temos que: $f(x) \in K_{k-1}[x]$ e $f^{\sigma^{k-1}}(x) = f^{\sigma}(x)$.

Aplicando a Proposição 2 para os corpos $K_{k-1} = K[\alpha_1, \dots, \alpha_{k-1}]$ e $K'_{k-1} = K'[\beta_1, \dots, \beta_{k-1}]$ com $\sigma_{k-1} : K_{k-1} \to K'_{k-1}$ temos que $\exists\, \beta$ (que denotaremos por $\beta_k$) raiz de $f^{\sigma}(x)$ e $\exists$ isomorfismo $\sigma_k : K_{k-1}[\alpha_k] \to$ $\to K'_{k-1}[\beta_k]$ tal que $\sigma_k|_{K_{k-1}} = \sigma_{k-1}$ e $\sigma_k(\alpha_k) = \beta_k$.

Daí segue que: $\exists\, \sigma_k : K[\alpha_1, \ldots, \alpha_k] \to K'[\beta_1, \ldots, \beta_k]$ isomorfismo tal que: $\sigma_i(\alpha_i) = \beta_i\ \forall\, i \in \{1, 2, \ldots, k\}$ e $\sigma_k|_K = \sigma$. Como $L = K_r = K[\alpha_1, \ldots, \alpha_r]$ o teorema segue imediatamente. ■

COROLÁRIO 1. *Seja $L \supset K$ uma extensão galoisiana e sejam $M, M'$ subcorpos de $L$ contendo $K$. Se $\sigma: M \to M'$ é um isomorfismo tal que $\sigma(a) = a\ \forall\, a \in K$ então $\exists\, \hat{\sigma} \in Aut_K\ L$ tal que $\hat{\sigma}|_M = \sigma$.*

*Demonstração.* Se $L = \mathrm{Gal}(f, K)$ então a demonstração é conseqüência direta do teorema anterior pois $f^{\sigma}(x) = f(x)$ e $L = \mathrm{Gal}(f, M) = L' = \mathrm{Gal}(f^{\sigma}, M')$. ■

COROLÁRIO 2. *Seja $L \supset K$ uma extensão finita. Então, $L \supset K$ galoisiana $\Leftrightarrow L \supset K$ normal.*

*Demonstração.* ($\Leftarrow$): Suponhamos $L \supset K$ normal. Como $L \supset K$ finita segue do Teorema 2 do Capítulo 5 que $L = K[u]$.

Agora como $L \supset K$ normal segue imediatamente que $L = \mathrm{Gal}(h, K)$ onde $h(x) = \mathrm{irr}(u, K)$.

($\Rightarrow$): Suponhamos agora $L \supset K$ galoisiana com $L = \mathrm{Gal}(f, K)$.

Seja $g(x) \in K[x]$ um polinômio irredutível tal que $\exists\, \alpha \in L$, $g(\alpha) = O$. Vamos provar que $\forall\, \beta \in \mathbb{C}$, $g(\beta) = O$ tem-se $\beta \in L$.

De fato,

Seja $\beta \neq \alpha$ uma raiz de $g(x)$ em $\mathbb{C}$. Sabemos pela Proposição 1 que $\exists\, \sigma: K[\alpha] \to K[\beta]$ isomorfismo tal que $\sigma(\alpha) = \beta$, e $\sigma(a) = a\ \forall\, a \in K$.

Sejam $M = K[\alpha]$, $M' = K[\beta]$ e $L' = \mathrm{Gal}(f, M')$.

Primeiramente observemos que, como $K \subset M \subset L$ e $K \subset M'$ temos

(1) $\quad L = \mathrm{Gal}(f, K) = \mathrm{Gal}(f, M)$.

(2) $\quad L = \mathrm{Gal}(f, K) \subset L' = \mathrm{Gal}(f, M')$.

Agora, $\sigma(a) = a\ \forall\, a \in K$ nos diz que $f^{\sigma} = f$ e, pelo Teorema 1, existe um isomorfismo

$$\hat{\sigma}: L = \mathrm{Gal}(f, M) \to L' = \mathrm{Gal}(f^{\sigma}, M')$$

tal que $\hat{\sigma}|_M = \sigma$, ou seja $\hat{\sigma}(a) = a\ \ \forall\, a \in K$.

Em particular temos,

(3) $\quad [L : K] = [L' : K]$.

Assim, (2) e (3) implicam que: $L = L'$ e isto termina a demonstração do Corolário 2 pois $\beta \in L'$.

COROLÁRIO 3. *Se $L \supset K$ galoisiana então* (a) $[L : K] = |Aut_K L|$.
(b) *Se $\alpha \in L - K \; \exists \, \sigma \in Aut_K L$ tal que $\sigma(\alpha) \neq \alpha$.*

*Demonstração.* (a) Seja $L = K[u]$. Se $h(x) = \text{irr}(u, K)$ então pelo corolário anterior $L = \text{Gal}(h(x), K)$ e $L$ contém todas as raízes de $h(x)$.

Se grau $h(x) = n$ temos $[L : K] = n$ e pela Proposição 2 do Capítulo 5 temos que $h(x)$ possui exatamente $n$ raízes distintas $u_1 = u, u_2, \ldots, u_n$.

Agora $\forall i \in \{1, 2, \ldots, n\} \; \exists$ isomorfismo (pela Proposição 1 deste capítulo) $\sigma_i : K[u] \to K[u_i]$ tal que $\sigma_i(u) = u_i$ e $\sigma_i(a) = a \; \forall a \in K$. Pelo Corolário 1 segue que $\exists \, \hat{\sigma}_i \in \text{Aut}_K L$ tal que $\hat{\sigma}_i|_{K[u]} = \sigma_i$, ou seja existem pelo menos $n$ automorfismos $\hat{\sigma}_1, \hat{\sigma}_2, \ldots, \hat{\sigma}_n \in \text{Aut}_K L$. Como, pelo Corolário 1 do Teorema 2 do Capítulo 5 $|\text{Aut}_K L| \leq [L : K] = n$ segue imediatamente a igualdade desejada.

(b) Seja $\alpha \in L, \alpha \notin K$. Se $g(x) = \text{irr}(\alpha, K)$ segue que grau $g(x) = r \geq 2$ e pela Proposição 2 do Capítulo 5, $\exists \, \beta \neq \alpha$ tal que $g(\beta) = 0$. Pelo Corolário 2 deste Capítulo $\beta \in L$ ($L$ é normal).

Agora pela Proposição 1 $\exists \, \sigma: K[\alpha] \to K[\beta]$ isomorfismo tal que $\sigma(a) = a \; \forall a \in K$ e $\sigma(\alpha) = \beta \neq \alpha$.

Pelo Corolário 1 $\exists \, \hat{\sigma} \in \text{Aut}_K L, \hat{\sigma}|_{K[\alpha]} = \sigma$ e isto demonstra o item (b). ∎

TEOREMA 2. *Se $L \supset M \supset K$ são extensões finitas e $L \supset K$ é Galoisiana, então as seguintes afirmações são equivalentes:*

(a) *$M \supset K$ galoisiana*
(b) *$\sigma(M) \subseteq M \; \forall \sigma \in Aut_K L$*
(c) *$Aut_M L \trianglelefteq Aut_K L$.*

*Demonstração.* (a) $\Rightarrow$ (b): Seja $u \in L$ tal que $M = K[u]$. Se $M \supset K$ galoisiana segue pelo Corolário 2 anterior que $M \supset K$ é uma extensão normal.

Agora, se $h = \text{irr}(u, K)$ e $\sigma \in \text{Aut}_K L$ sabemos que $v = \sigma(u)$ é também raiz de $h(x)$ e pela normalidade de $M \supset K$ temos $v = \sigma(u) \in M$, ou seja, $\sigma(K[u]) \subseteq K[u]$ como queríamos demonstrar.

(b) $\Rightarrow$ (a): Seja $u \in L$ tal que $M = K[u]$ e seja $h = \text{irr}(u, K)$. Vamos provar que se $\sigma(M) \subseteq M \; \forall \, \sigma \in \text{Aut}_K L$ temos $M = \text{Gal}(h, K)$.

Seja $v$ raiz de $h(x)$, e seja $M' = K[v]$. Pela Proposição 1 existe isomorfismo, $\sigma_0 : M \to M'$ tal que

$$\sigma(u) = v \text{ e } \sigma(a) = a \ \forall\, a \in K.$$

Pelo Teorema 1 existe $\sigma \in \text{Aut}_K L$ tal que $\sigma|_M = \sigma_0$. Como $\sigma(M) \subseteq M$ e $u \in M$ teremos $v = \sigma(u) \in M$ e isto prova a implicação $(b) \Rightarrow (a)$.

$(b) \Rightarrow (c)$: Sejam $\sigma \in \text{Aut}_K L$ e $\gamma \in \text{Aut}_M L$. Vamos provar que se $\sigma(M) \subseteq M$ então $\sigma^{-1} \circ \gamma \circ \sigma \in \text{Aut}_M L$.

De fato, se $\sigma(M) \subseteq M$ e $m' = \sigma(m)$, $m \in M$ temos:

$$\gamma(m') = m' \text{ e } (\sigma^{-1} \circ \gamma \circ \sigma)(m) = \sigma^{-1}(\gamma(m')) = \sigma^{-1}(m') = m$$

e isto demonstra a implicação $(b) \Rightarrow (c)$.

$(c) \Rightarrow (b)$: Suponhamos por absurdo que. $\exists\, \sigma \in \text{Aut}_K L$ e $\exists\, u \in M$ tal que $\sigma(u) = v \notin M$. Como $L \supset K$ Galoisiana temos $L \supset M$ galoisiana e pelo Corolário 3, item (b), segue que: $\exists\, \gamma \in \text{Aut}_M L$ tal que $\gamma(v) \neq v$.

Assim, $(\sigma^{-1} \circ \gamma \circ \sigma)(u) = \sigma^{-1}(\gamma(v)) \neq \sigma^{-1}(v) = u$ ou seja $\sigma^{-1} \circ \gamma \circ \sigma \notin \text{Aut}_M L$ contrariando a hipótese $\text{Aut}_M L \trianglelefteq \text{Aut}_K L$. ∎

TEOREMA 3. *Seja $L \supset K$ uma extensão finita. Então as seguintes condições são equivalentes:*

(1) *$L \supset K$ galoisiana.*
(2) *$L \supset K$ normal*
(3) *$\forall\, \alpha \in L - K \ \exists\, \sigma \in Aut_K L$ tal que $\sigma(\alpha) \neq \alpha$.*
(4) *$[L:K] = |Aut_K L|$*

*Demonstração.* $(1) \Rightarrow (2)$: segue imediatamente do Corolário 2 do Teorema 1.

$(2) \Rightarrow (3)$: segue imediatamente dos Corolário 2 e 3 do Teorema 1.

$(3) \Rightarrow (4)$: Sabemos do Corolário 1 do Teorema 2 do Capítulo 5 que $[L:K] \geq |\text{Aut}_K L|$. Suponhamos (3) e, por absurdo, $[L:K] > |\text{Aut}_K L|$.

Seja $\text{Aut}_K L = \{\varphi_1 = I_L, \varphi_2, \varphi_3, \ldots, \varphi_n\}$ onde $I_L$ representa o automorfismo identidade de $L$.

Se $[L:K] > n$ então $\exists\ u_1, u_2, \ldots, u_n, u_{n+1} \in L$ linearmente independentes sobre o corpo $K$:

Consideremos agora o seguinte sistema linear homogêneo com $n$ equações e $(n + 1)$ incógnitas $a_1, a_2, \ldots, a_{n+1}$ em $L$:

$$(*)\begin{cases} \varphi_1(u_1)a_1+\varphi_1(u_2)a_2+\ldots+\varphi_1(u_j)a_j+\ldots+\varphi_1(a_n)a_n+\varphi_1(u_{n+1})a_{n+1}=0\\ \varphi_2(u_1)a_1+\varphi_2(u_2)a_2+\ldots+\varphi_2(u_j)a_j+\ldots+\varphi_2(a_n)a_n+\varphi_2(u_{n+1})a_{n+1}=0\\ \vdots \\ \varphi_i(u_1)a_1+\varphi_i(u_2)a_2+\ldots+\varphi_i(u_j)a_j+\ldots+\varphi_i(u_n)a_n+\varphi_i(u_{n+1})a_{n+1}=0\\ \vdots \\ \varphi_n(u_1)a_1+\varphi_n(u_2)a_2+\ldots+\varphi_n(u_j)a_j+\ldots+\varphi_n(u_n)a_n+\varphi_n(u_{n+1})a_{n+1}=0 \end{cases}$$

Como o número de equações de $(*)$ é menor do que o número de incógnitas então $(*)$ admite uma solução $a_1, a_2, \ldots, a_{n+1}$ não todos nulos.

Consideremos agora uma solução não trivial de $(*)$ com o maior número de zeros possível e denotaremos os $a_i's$ não nulos dessa solução por $a_1, a_2, \ldots, a_r$.

Multiplicando por $a_1^{-1}$ se necessário podemos assumir que $a_1 = 1$. Assim $1, a_2, a_3 \ldots, a_r$ não nulos são tais que $1\ a_2\ a_3\ \ldots\ a_r\ 0 \ldots 0$ é uma solução de $(*)$ com um número máximo de valores zeros. Então temos,

$$\forall\, i \in \{1, 2, \ldots, n\}, \varphi_i(u_1) + \varphi_i(u_2)a_2 + \ldots + \varphi_i(u_r)a_r = 0.$$

Como $\varphi_1 = I_L$ e $u_1, \ldots, u_r, \ldots, u_n$ são linearmente independentes sobre $K$ então segue que $\exists\, a_i \in L$ tal que $a_i \notin K$. Seja $a_r \notin K$. Assim por (3) $\exists\, \sigma \in \mathrm{Aut}_K L$ tal que:

$$\sigma(a_r) \neq a_r.$$

Daí segue que:

$$\forall\, i \in \{1, 2, \ldots, n\},$$

$$(\sigma \circ \varphi_i)(u_1) + (\sigma \circ \varphi_i)(u_2) \cdot \sigma(a_2) + \ldots + (\sigma \circ \varphi_i)(u_r) \cdot \sigma(a_r) = 0.$$

Como $\mathrm{Aut}_K\, L$ é um grupo e $\sigma \in \mathrm{Aut}_K\, L$ segue imediatamente que:

$$\mathrm{Aut}_K\, L = \{\varphi_1, \varphi_2, \ldots, \varphi_n\} = \{\sigma\varphi_1, \sigma\varphi_2, \ldots, \sigma\varphi_n\}$$

Portanto se $\sigma\varphi_i = \varphi_k$ teremos,

$$\forall\, k \in \{1, 2, \ldots, n\},$$

$$\varphi_k(u_1) + \varphi_k(u_2)\sigma(a_2) + \ldots + \varphi_k(u_r)\sigma(a_r) = 0$$

$$\forall\, i \in \{1, 2, \ldots, n\},$$

$$\varphi_i(u_1) + \varphi_i(u_2)a_2 + \ldots + \varphi_i(u_r)a_r = 0$$

Daí segue que:

$$\forall\, j \in \{1, 2, \ldots, n\}$$

$$\varphi_j(u_2)(\sigma(a_2) - a_2) - a_2) + \ldots + \varphi_j(u_r)(\sigma(a_r) - a_r) - a_r) = 0$$

Como $\sigma(a_r) - a_r \neq 0$ temos uma contradição pela nossa escolha dos $a_i$'s com número máximo de zeros e isto demonstra que (3) $\Rightarrow$ (4).

(4) $\Rightarrow$ (1): Suponhamos $L \supset K$ extensão finita e $[L:K] = |\text{Aut}_K L|$. Vamos provar que $L \supset K$ é galoisiana.

Seja $L = K[u]$. Sabemos que se $h(x)$ é definido por $h = \text{irr}(u, K)$ então $\forall\, \sigma \in \text{Aut}_K L$ tem-se $\sigma(u) \in L$ e $\sigma(u)$ raiz de $h(x)$. Assim, $|\text{Aut}_K L|$ é menor ou igual ao número de raízes de $h(x)$ em $L$. Agora, se $[L:K] = |\text{Aut}_K L|$ então $|\text{Aut}_K L| =$ grau de $h(x)$ e portanto igual ao número de raízes de $h(x)$ em $L$. Daí segue imediatamente que $L$ contém todas as raízes de $h(x)$, ou seja, $L = \text{Gal}(h, K)$ como queríamos demonstrar. ■

Antes de encerrar esse parágrafo vamos ver alguns resultados úteis na determinação da estrutura do grupo $G = \text{Aut}_K L$.

**PROPOSIÇÃO 3.** *Se $L \supset K$ é uma extensão galoisiana de grau $n$ então $G = \text{Aut}_K L$ é isomorfo a um subgrupo de $S_n$.*

**COROLÁRIO 1.** *Se $L = \text{Gal}(x^3 - 2, \mathbb{Q})$ então $\text{Aut}_{\mathbb{Q}} L \simeq S_3$.*

*Demonstração do Corolário* 1. Pelo Corolário 3 da Proposição 4 do Capítulo 5 sabemos que $[L:\mathbb{Q}] = 6$ onde $L = \text{Gal}(x^3 - 2, \mathbb{Q})$ e portanto $|\text{Aut}_{\mathbb{Q}} L| = 6$ e como $|S_3| = 6$ o corolário segue imediatamente da Proposição 3. ■

*Demonstração da Proposição* 3. Seja $L = K[u]$, $h = \text{irr}(u, K)$, $[L:K] =$ grau $h(x) = n$, e $\Omega = \{u_1 = u, u_2, \ldots, u_n\}$ o conjunto de todas as raízes complexas de $h(x)$. Como $L \supset K$ galoisiana temos $\Omega \subset L$. Sabemos também que $\forall\, \sigma \in G = \text{Aut}_K L$ e $\forall\, u_i \in \Omega$ tem-se $\sigma(u_i) \in \Omega$ e como $\Omega$ é um conjunto finito e $\sigma$ injetiva segue que $\sigma_0 = \sigma|_\Omega : \Omega \to \Omega$ define uma permutação do conjunto $\Omega$. Se $\mathscr{P}(\Omega)$ denota o grupo das permutações do conjunto $\Omega$ então é suficiente provarmos que $G$ é isomorfo a um subgrupo de $\mathscr{P}(\Omega)$ pois $\mathscr{P}(\Omega) \simeq S_n$.

Agora, é fácil verificar que (prove isto) a seguinte função $\psi$ define um homomorfismo de grupos, pois $(\sigma \circ \tau)|_\Omega = \sigma|_\Omega \cdot \tau|_\Omega$.

$$\begin{aligned} \psi: G &\to \mathscr{P}(\Omega) \\ \sigma &\leadsto \sigma_0 = \sigma|_\Omega \end{aligned}$$

Mais ainda, se $\sigma_0 = \sigma|_\Omega = I_\Omega$ (identidade em $\Omega$) segue que $\sigma(u) = u$ e isto nos diz que $\sigma = I_L$, pois $\forall\, b \in L$, $b = a_0 + a_1 u + \ldots + a_{n-1} u^{n-1}$,

onde $a_i \in K$ e $\forall\, \sigma \in G = \text{Aut}_K\, L$ tem-se: $\sigma(b) = a_0 + a_1\sigma(u) + \ldots + a_{n-1}\sigma(u)^{n-1} = a_0 + \ldots + a_{n-1}u^{n-1} = b$.

Portanto $\psi$ é injetiva e portanto pelo 1.º teorema de isomorfismo de grupos temos, $G \simeq \psi(G) \leq \mathscr{P}(\Omega)$ como queríamos demonstrar. ■

**PROPOSIÇÃO 4.** *Se $L = \text{Gal}(x^n - 2, K)$ onde $K \supset \mathbb{Q}$ contém uma raiz $\zeta$ primitiva, n-ésima, da unidade, então $G = \text{Aut}_K L$ é um grupo abeliano.*

*Demonstração.* Seja $\alpha = \sqrt[n]{2} \in \mathbb{R}$ e $\zeta = \cos\dfrac{2\pi}{n} + i\,\text{sen}\,\dfrac{2\pi}{n}$ então $\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}$ são as $n$ distintas raízes de $x^n - 2$ em $\mathbb{C}$.

Sabemos que $L = K[\alpha, \zeta] = K[\zeta, \alpha] = K[\alpha]$ pois $\zeta \in K$.

Assim, se $\sigma, \tau \in \text{Aut}_K L$ eles são determinados completamente pelos valores $\sigma(\alpha)$ e $\tau(\alpha)$. Ora, $\sigma, \tau \in \text{Aut}_K L \Rightarrow \sigma(\alpha) = \alpha\zeta^i$ para algum $i$ e $\tau(\alpha) = \alpha\zeta^j$ para algum $j$. Daí segue, considerando $\zeta \in K$, que:

$$(\sigma \circ \tau)(\alpha) = \sigma(\alpha\zeta^j) = \sigma(\alpha)\zeta^j = \alpha\zeta^{i+j}$$

$$(\tau \circ \sigma)(\alpha) = \tau(\alpha\zeta^i) = \tau(\alpha)\zeta^i = \alpha\zeta^{j+i}.$$

Assim $\sigma \circ \tau(\alpha) = \tau \circ \sigma(\alpha)\ \forall\, \sigma, \tau \in G = \text{Aut}_K L$ e isto prova a proposição pois como $L = K[\alpha]$ os automorfismos $\gamma$ em $G = \text{Aut}_K\, L$ são determinados pelos valores $\gamma(\alpha)$. ■

**PROPOSIÇÃO 5.** *Seja $p$ um número primo e $f(x) \in Q[x]$ um polinômio irredutível sobre $\mathbb{Q}$ de grau $p$. Se $f(x)$ possui exatamente duas raízes não reais então $Aut_{\mathbb{Q}}\, L \simeq S_p$ onde $L = Gal(f, \mathbb{Q})$.*

*Demonstração.* Seja $L = \text{Gal}(f, \mathbb{Q})$. Como grau $f(x) = p$ e $f(x)$ irredutível sobre $\mathbb{Q}, f(x)$ possui exatamente $p$ raízes distintas e pela Proposição 3 $G = \text{Aut}_{\mathbb{Q}}\, L$ é isomorfo a um subgrupo $H$ de $S_p$.

Se $\alpha$ é uma raiz de $f(x)$ então $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset L$ e $|G| = |H| = [L:\mathbb{Q}] = [L:\mathbb{Q}[\alpha]][\mathbb{Q}[\alpha]:\mathbb{Q}]$. Portanto $[\mathbb{Q}[\alpha]:\mathbb{Q}] = p$ divide $|H|$. Como $H \leq S_p$ segue imediatamente pelo Teorema de Cauchy que $\exists\, a \in H$ tal que $\mathcal{O}(a) = p$. Como $a \in S_p$ a só pode ser um p-ciclo. Sem perda de generalidade vamos denotar $a = (1, 2, \ldots, p)$.

Se $K = \mathbb{Q}[\alpha_1, \ldots, \alpha_{p-2}]$ onde $\alpha_1, \ldots, \alpha_{p-2}$ são as raízes reais de $f(x)$ então segue imediatamente que $L = K[\beta]$ onde $\beta$ é uma raiz complexa de $f(x)$. Claramente $\exists\, \sigma \in \text{Aut}_K\, L$ tal que $\sigma(\beta) = \bar{\beta}$ pois

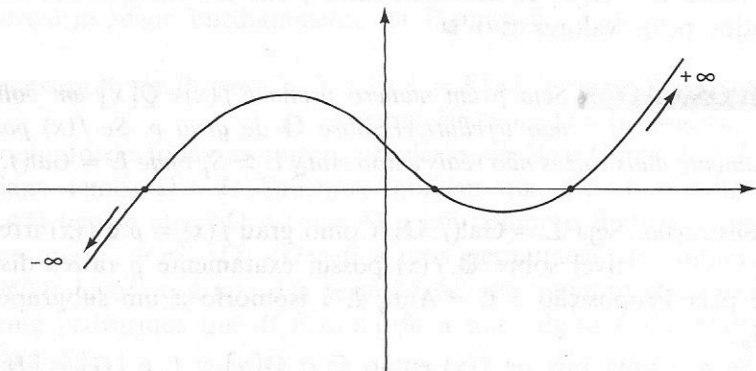
$[L:K] = |\mathrm{Aut}_K L| = 2$ e $\beta$, $\bar{\beta}$ são as raízes complexas, não reais, de $f(x)$ e $\bar{\beta}$ é o complexo conjugado de $\beta$. Portanto, $\sigma \in \mathrm{Aut}_{\mathbb{Q}} L$ e $\sigma(\alpha_i) = \alpha_i$ $\forall\, i = 1, \ldots, p-2$, e $\sigma(\beta) = \bar{\beta}$. Renumerando os índices das raízes se necessário segue que a imagem de $\sigma$ em $S_p$ é uma transposição que podemos notar por $(12) \in H$.

Ora $(1, 2, \ldots, p)$ e $(12) \in H \leq S_p$ implica pelo Corolário da Proposição 14 do Capítulo 6 que $G \simeq H = S_p$ como queríamos demonstrar. ■

COROLÁRIO. *Seja $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ e $L = Gal(f, \mathbb{Q})$. Então $G = Aut_{\mathbb{Q}} L \simeq S_5$. Em particular $Aut_{\mathbb{Q}} L$ não é um grupo solúvel.*

*Demonstração.* Pelo critério de Eisenstein $f(x)$ é irredutível sobre $\mathbb{Q}$.

Como grau $f(x) = 5$ é um número primo, é suficiente provarmos que $f(x)$ possui exatamente 3 raízes reais.

Agora, com a ajuda do cálculo, observando também os valores: $f(-2) = -17$, $f(-1) = 8$, $f(6) = 3$, $f(1) = -2$ e $f(2) = 23$, $f(x)$ como função real possui um gráfico do tipo abaixo, o que demonstrar o corolário: ■

Antes de encerrarmos esse parágrafo, vamos calcular $G = \mathrm{Aut}_K L$, em alguns casos particulares.

EXEMPLO 1. Seja $L = \mathrm{Gal}(x^4 - 2, \mathbb{Q})$. Seja $\alpha = \sqrt[4]{2}$. Como $x^4 - 1$ fatora-se em $x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)$ temos imediatamente que $L = \mathbb{Q}[\alpha, i]$ onde $i^2 = -1$.

Assim, $[L:\mathbb{Q}] = |\text{Aut}_{\mathbb{Q}} L| = 8$. Vamos calcular os 8 elementos de $G = \text{Aut}_{\mathbb{Q}} L$ e provaremos que $G$ é um grupo não abeliano de ordem 8 (mais precisamente $G \simeq D_4$).

Sabemos que $\forall \sigma \in G$, $\sigma$ fica determinado completamente pelos vetores $\sigma(\alpha)$ e $\sigma(i)$, já que $1, \alpha, \alpha^2, \alpha^3, i, \alpha i, \alpha^2 i, \alpha^3 i$ é uma base de $L$ sobre $\mathbb{Q}$.

Agora, sabemos que: $\forall \sigma \in G$ $\sigma(\alpha)^4 = 2$ e $\sigma(i)^2 = -1$. Assim, se $\sigma \in G$ as possibilidades para $\sigma(\alpha)$ são $\alpha, -\alpha, \alpha i, -\alpha i$, e para $\sigma(i)$ são $i, -i$, e $G$ é então determinado pelo quadro abaixo:

| | $I_L$ | $\sigma_2$ | $\sigma_3$ | $\sigma_4$ | $\sigma_5$ | $\sigma_6$ | $\sigma_7$ | $\sigma_8$ |
|---|---|---|---|---|---|---|---|---|
| $\alpha \to$ | $\alpha$ | $\alpha$ | $-\alpha$ | $-\alpha$ | $\alpha i$ | $\alpha i$ | $-\alpha i$ | $-\alpha i$ |
| $i \to$ | $i$ | $-i$ | $i$ | $-i$ | $i$ | $-i$ | $i$ | $-i$ |

É fácil observar que $\sigma_5$ e $\sigma_7$ são os únicos elementos de ordem 4, enquanto que os demais, diferentes de $I_L$, possuem ordem 2. Observe também que:

$$(\sigma_5 \circ \sigma_6)(\alpha) = \sigma_5(\alpha i) = \sigma_5(\alpha)\sigma_5(i) = (2i)i = -\alpha$$
$$(\sigma_6 \circ \sigma_5)(\alpha) = \sigma_6(\alpha i) = \sigma_6(\alpha)\sigma_6(i) = (\alpha i) \cdot -i = \alpha.$$

ou seja $\sigma_5 \circ \sigma_6 \neq \sigma_6 \circ \sigma_5$ e $G$ é não abeliano de ordem 8. Como $\mathbb{Q}_8$ (quaternios de ordem 8) possui um único elemento de ordem 2 então segue que $G \simeq D_4$, o grupo dihedral de ordem 8. Para isso observe que:

$$G = \langle \sigma_5, \sigma_2 : \sigma_5^4 = \sigma_2^2 = I_L, \sigma_2 \cdot \sigma_5 = \sigma_5^{-1} \cdot \sigma_2 \rangle$$

EXEMPLO 2. Seja $h(x) = x^3 + px + q \in \mathbb{Q}[x]$ *um* polinômio irredutível sobre $\mathbb{Q}$, e seja $D = -4p^3 - 27q^2 \in \mathbb{Q}$. Denotaremos $L = \text{Gal}(h, \mathbb{Q})$ e $G = \text{Aut}_{\mathbb{Q}} L$.

Se $\{\alpha_1, \alpha_2, \alpha_3\} = \Omega$ é o conjunto das 3 raízes (distintas) de $h(x)$ sabemos que:

$$(*) \quad \begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p \\ \alpha_1\alpha_2\alpha_3 = -q \end{cases}$$

Seja $\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in L$. Usando as relações (*) acima pode-se provar que:

$$D = \Delta^2, \text{ i.e., } \Delta = \sqrt{D} \text{ onde } D = -4p^3 - 27q^2.$$

Sabemos que podemos identificar $G$ (através de um isomorfismo) com um subgrupo do grupo $\mathscr{P}(\Omega) \simeq S_3$ das permutações do conjunto $\Omega$.

Se $\Delta = \sqrt{D} \in \mathbb{Q}$ temos que $\Delta^\sigma = \Delta \ \forall \sigma \in G$, ou seja, as permutações induzidas pelos elementos de $G$ são todas pares pois $\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$.

Como $[L:\mathbb{Q}] \geq 3$ temos imediatamente nesse caso que,

$$G \simeq A_3.$$

Se $\Delta = \sqrt{D} \notin \mathbb{Q}$ então $\mathbb{Q}[\sqrt{D}] \subseteq L$ pois $\Delta = \sqrt{D} \in L$, e daí segue que 2 divide $[L:\mathbb{Q}]$. Como evidentemente 3 divide $[L:\mathbb{Q}]$ temos nesse caso que $G \simeq S_3$.

Em particular, se $h(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$ temos que $h(x)$ é irredutível sobre $\mathbb{Q}$.

Como $\Delta = \sqrt{D} = \sqrt{81} \in \mathbb{Q}$ segue que nesse caso particular tem-se $G \simeq A_3$, e portanto $L$ é uma extensão galoisiana de grau 3 sobre $\mathbb{Q}$.

EXERCÍCIOS

1. Prove que:
   Se $L \supset K$ é tal que $[L:K] = 2$ então $L \supset K$ é galoisiana.
2. Prove que:
   Se $L = \text{Gal}(x^n - 1, \mathbb{Q})$ então $\text{Aut}_{\mathbb{Q}} L$ é abeliano.
3. Prove que:
   Se $a \in K$, $L = \text{Gal}(x^n - a, K)$ e $K$ contém uma raiz primitiva n-ésima da unidade, então $\text{Aut}_K L$ é abeliano.
4. Calcule $\text{Aut}_{\mathbb{Q}} L$ para as seguintes extensões $L$ abaixo:
   a) $L = \mathbb{Q}[\alpha]$, $\alpha = \sqrt[5]{3} \in \mathbb{R}$.
   b) $L = \mathbb{Q}[\alpha]$, $\alpha = \sqrt[7]{2} \in \mathbb{R}$.
   c) $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$
   d) $L = \mathbb{Q}[u]$, $u$ é raiz de $x^3 - 3x^2 + 3 \in \mathbb{Q}[x]$
   e) $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$.
   f) $L = \mathbb{Q}[\sqrt{2}, \sqrt[3]{5}]$

5. Prove que:
$\mathbb{Q}[\sqrt[4]{2}]$ é normal sobre $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{2}]$ é normal sobre $\mathbb{Q}$ mas $\mathbb{Q}[\sqrt[4]{2}]$ não é normal sobre $\mathbb{Q}$.
6. Dê exemplo de extensão $L \supset \mathbb{Q}, L \not\subseteq \mathbb{R}$ tais que:
a) $L \simeq \mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$.
b) $L \simeq \mathbb{Q}[\sqrt[3]{3}] \subseteq \mathbb{R}$.
c) $L \simeq \mathbb{Q}[\sqrt[4]{5}] \subseteq \mathbb{R}$.
7. Seja $L = \text{Gal}(x^3 - 2, \mathbb{Q})$. Calcule todos os corpos intermediários $N, L \supset N \supset \mathbb{Q}$ tais que $N \supset \mathbb{Q}$ é uma extensão normal.
8. Mesmo exercício do item anterior para a extensão $L = \text{Gal}(x^4 - 2, \mathbb{Q})$.

## §2 A correspondência de Galois

Seja $M \supset K$ uma extensão finita. Dizemos que $L$ é um *corpo intermediário de* $M \supset K$ se $L$ é um subcorpo de $M$ contendo $K$, ou seja, $M \supset L \supset K$.

Se $G = \text{Aut}_K M$ usaremos as seguintes notações:

$$\mathscr{I}(M, K) = \{L : \text{ corpo intermediário de } M \supset K\}$$
$$\mathscr{S}(G) = \{H : H \text{ subgrupo de } G\}.$$

Se $H \in \mathscr{S}(G)$ então $L = \{a \in M : \gamma(a) = a \quad \forall \gamma \in H\}$ é um corpo intermediário de $M \supset K$. De fato, obviamente $0, 1 \in L$ e mais:
(i) se $x, y \in L$ então $\gamma(x - y) = \gamma(x) - \gamma(y) = x - y, \ \forall \gamma \in H$.
(ii) se $x, y \in L$ então $\gamma(xy) = \gamma(x) \cdot \gamma(y) = xy, \ \forall \gamma \in H$
e
(iii) se $x \in L, x \neq 0$ então $\gamma(x^{-1}) = \gamma(x)^{-1} = x^{-1} \ \forall \gamma \in H$
e como $G = \text{Aut}_K M$ e $H \leq G$ segue imediatamente que $L$ é um corpo, $M \supset L \supset K$. Esse corpo $L$ é chamado de *corpo fixo de* $H$.

Consideremos agora as seguintes correspondências:

$$\mathscr{I}(M, K) \overset{\psi}{\to} \mathscr{S}(G),$$
$$L \rightsquigarrow \psi(L) = \text{Aut}_L M,$$

$$\mathscr{S}(G) \overset{\theta}{\to} \mathscr{I}(M, K)$$
$$H \rightsquigarrow \theta(H) = \{a \in M : \gamma(a) = a \ \forall \gamma \in H\}, \text{ o corpo fixo de } H.$$

Observemos agora algumas propriedades elementares dessas correspondencias

(1) $\psi(K) = \text{Aut}_K M = G$

(2) $\psi(M) = \text{Aut}_M M = \{I_M\}$

(3) $\theta(\{I_M\}) = \{a \in M : I_M(a) = a\} = M$

(4) $\theta(G) = \{a \in M : \gamma(a) = a \ \ \forall \gamma \in G\} \supseteq K$, e pelo Teorema 3 temos ainda que:

$$\theta(G) = K \Leftrightarrow M \supset K \text{ galoisiana.}$$

PROPOSIÇÃO 6. *Mantendo as notações acima, temos*: (a) *se* $L_1, L_2 \in \mathscr{I}(M, K)$ *e* $L_1 \subseteq L_2$ *então* $\psi(L_1) \geq \psi(L_2)$

(b) *se* $H_1, H_2 \in \mathscr{S}(G)$ *e* $H_1 \leq H_2$ *então* $\theta(H_1) \supseteq \theta(H_2)$

(c) $\forall L \in \mathscr{I}(M, K)$ *tem-se* $(\theta \circ \psi)(L) \supseteq L$.

(d) $\forall H \in \mathscr{S}(G)$ *tem-se* $(\psi \circ \theta)(H) \geq H$.

*Demonstração.* (a) Sejam $L_1, L_2 \in \mathscr{I}(M, K)$ e $L_1 \subset L_2$. Então,

$$\psi(L_1) = \text{Aut}_{L_1} M \geq \text{Aut}_{L_2} M = \psi(L_2)$$

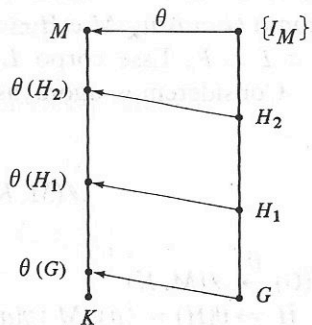
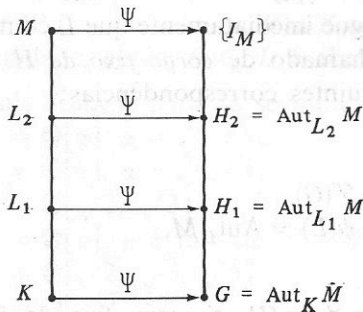
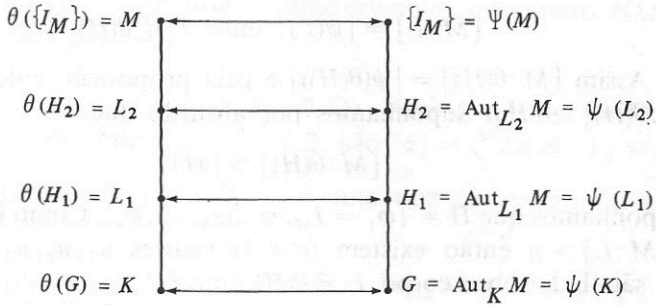
(b) Sejam $H_1, H_2 \in \mathscr{S}(G)$ e $H_1 \leq H_2$. Então,

$$\theta(H_2) = \{a \in M : \gamma(a) = a \ \forall \gamma \in H_2\} \subseteq \{a \in M : \gamma(a) = a \ \forall \gamma \in H_1\} = \theta(H_1)$$

(c) Seja $L \in \mathscr{I}(M, K)$. Como $\psi(L) = \text{Aut}_L M$ a inclusão $L \subseteq (\theta \circ \psi)(L)$ segue imediatamente das nossas definições.

(d) Seja $H \in \mathscr{S}(G)$ Se $N = \theta(H) = \{a \in M : \gamma(a) = a \ \forall \gamma \in H\}$ então segue imediatamente que $H \leq \text{Aut}_N M = \psi(\theta(H))$ e isto demonstra a Proposição 6. ■

As figuras abaixo nos dão uma idéia gráfica das correspondências $\psi$ e $\theta$ (invertendo a ordem inclusão). Nas figuras estamos também considerando,

$$K \subseteq L_1 \subseteq L_2 \subseteq M \text{ e } \{I_M\} \leq H_2 \leq H_1 \leq G = \text{Aut}_K M.$$

Nós provaremos a seguir que se $M \supset K$ é uma extensão galoisiana então $\psi \circ \theta = I_{\mathscr{S}(G)}$ e $\theta \circ \psi = I_{\mathscr{S}(M,K)}$, ou seja, $\psi$ é bijetiva (tendo $\theta$ como inversa) e portanto existe uma correspondência bijetiva entre $\mathscr{I}(M, K)$ e $\mathscr{S}(G)$, chamada *correspondência de Galois da extensão* $M \supset K$. Nesse caso temos a seguinte representação gráfica:

Agora vamos demonstrar o Teorema fundamental da Teoria de Galois para extensões $M \supset K \supset \mathbb{Q}$. Para isso vamos manter as notações desse parágrafo.

TEOREMA 4 (Teorema Fundamental de Galois). *Se $M \supset K$ é uma extensão galoisiana, então:*

(a) $\forall\, L \in \mathscr{I}(M, K)$ *tem-se* $[M:L] = |\psi(L)|$ *e* $[L:K] = [G:\psi(L)]$ *(o índice de $\psi(L)$ em $G$)*

(b) $\forall\, H \in \mathscr{S}(G)$ *tem-se* $[M:\theta(H)] = |H|$ *e* $[\theta(H):K] = [G:H]$ *(o índice de $H$ em $G$)*

(c) $\psi \circ \theta = I_{\mathscr{S}(G)}$ *e* $\theta \circ \psi = I_{\mathscr{I}(M,K)}$

(d) $\forall\, L \in \mathscr{I}(M, K)$, $L \supset K$ *galoisiana* $\Leftrightarrow \psi(L) = Aut_L\, M \trianglelefteq G$.

(e) *Seja* $L \in \mathscr{I}(M, K)$. *Se* $L \supset K$ *galoisiana então* $[L:K] = |Aut_K\, L|$ *e* $G/\psi(L) \simeq Aut_K\, L$.

*Demonstração.* (a) Seja $L \in \mathscr{I}(M, K), M \supset L \supset K$

Ora $M \supset K$ galoisiana implica que $M \supset L$ é galoisiana e pelo Teorema 3 segue que:

$$[M:L] = |\text{Aut}_L\, M| = |\psi(L)|$$

e como $[M:K] = |\text{Aut}_K\, M| = [M:L] \cdot [L:K]$ nós temos que:

$$|G| = [M:L] \cdot [L:K] = |\psi(L)| \cdot [L:K]$$

e daí vem que: $[L:K] = [G:\psi(L)]$ como queríamos demonstrar.

(b) Sejam $H \leq G$ e $L = \theta(H)$. Como $|G| = [M:K] = [M:\theta(H)] \cdot$ $\cdot [\theta(H):K]$ então a fórmula $[\theta(H):K] = [G:H]$ segue imediatamente da primeira parte $[M:\theta(H)] = |H|$ e é essa que vamos demonstrar a seguir. Vamos praticamente repetir o argumento usado no Teorema 3.

Sabemos pelo item (a) que:

$$[M:L] = |\psi(L)| \text{ onde } L = \theta(H).$$

Assim $[M:\theta(H)] = |\psi(\theta(H))|$ e pela proposição anterior tem-se: $[M:\theta(H)] \geq |H|$. Suponhamos por absurdo que:

$$[M:\theta(H)] > |H|$$

e suponhamos que $H = \{\varphi_1 = I_M, \varphi_2, \varphi_3, \ldots, \varphi_n\}$. Como $[M:\theta(H)] =$ $= [M:L] > n$ então existem $(n+1)$ vetores $u_1, u_2, u_3, \ldots, u_n, u_{n+1}$ que são L. I. sobre corpo $L = \theta(H)$.

Agora de modo totalmente análogo ao que fizemos no Teorema 3 chegamos a uma contradição e o item b está demonstrado.

(c) Seja $H \in \mathscr{S}(G)$ e $L \in \mathscr{I}(M, K)$. Sabemos da proposição anterior que:

$$H \leq \psi(\theta(H)) \text{ e } L \leq \theta(\psi(L)).$$

Pelo item (a), temos: $[G:\psi(\theta(H))] = [\theta(H):K]$ e pelo item (b), temos: $[\theta(H):K] = [G:H]$. Daí segue imediatamente que $\psi(\theta(H)) = H$. Analogamente, pelo item (b): $[M:\theta(\psi(L))] = |\psi(L)|$ e pelo item (a) temos $|\psi(L)| = [M:L]$. Daí segue imediatamente que:

$$\theta \circ (\psi(L)) = L.$$

Portanto fica demonstrado o item (c).

(d) Conseqüência imediata do Teorema 2.

(e) Pelo item (a) sabemos que $[G:\psi(L)] = [L:K]$ portanto é suficiente provarmos que: $\forall\, L \in \mathscr{I}(M, K)\; L \supset K$ galoisiana implica que:

$$G/\psi(L) \simeq \mathrm{Aut}_K L.$$

De fato, como $L \supset K$ galoisiana sabemos do Teorema 2 que, $\forall\, \sigma \in G = \mathrm{Aut}_K M$ tem-se $\sigma_0 = \sigma|_L \in \mathrm{Aut}_K L$, portanto podemos definir a seguinte função:

$$\begin{aligned} \Phi: G &\to \mathrm{Aut}_K \mathrm{L} \\ \sigma &\leadsto \sigma_0 = \sigma|_L \end{aligned}$$

$\Phi$ é evidentemente um homomorfismo de grupos, cujo núcleo $N(\Phi) =$
$= \{\sigma \in G : \sigma_0 = \sigma|_L = I_L\} = \text{Aut}_L M = \psi(L)$.

Agora pelo Teorema da extensão sabemos que $\Phi$ é também sobrejetiva e o resto segue do 1.º teorema de isomorfismo. ■

Antes de encerrar esse parágrafo vamos usar o teorema fundamental de Galois para calcularmos, como exemplos, o conjunto $\mathscr{I}(M, K)$ em alguns casos particulares.

EXEMPLO 1. Seja $M = \text{Gal}(x^3 - 2, \mathbb{Q})$. Vamos calcular $\mathscr{I}(M, \mathbb{Q})$.
As raízes de $x^3 - 2$ são $\alpha_1 = \sqrt[3]{2} \in \mathbb{R}$, $\alpha_2 = \alpha_1\zeta$, $\alpha_3 = \alpha_1\zeta^2$ onde $\zeta = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}\, i$ é uma raiz cúbica primitiva da unidade.

Se $\Omega = \{\alpha_1, \alpha_2, \alpha_3\}$ sabemos que $G = \text{Aut}_{\mathbb{Q}} M \simeq \mathscr{P}(\Omega)$ grupo das permutações de $\Omega$. Se denotarmos essas permutações como ciclos então os 6 elementos de $G$, como permutação de $\Omega$, são:

$$e = I_\Omega,\ (\alpha_1\alpha_2),\ (\alpha_1\alpha_3),\ (\alpha_2\alpha_3),\ (\alpha_1\alpha_2\alpha_3),\ (\alpha_1\alpha_3\alpha_2)$$

e os subgrupos de $G$ são:

$$G, \{e\}, \{e, (\alpha_2\alpha_3)\} = A_1, \{e, (\alpha_1\alpha_2)\} = A_2,$$
$$\{e, (\alpha_1\alpha_2)\} = A_3 \text{ e } B = \{e, (\alpha_1\alpha_2\alpha_3), (\alpha_1\alpha_3\alpha_2)\}.$$

Pelo teorema fundamental de Galois os corpos $L$, intermediários de $M \supset \mathbb{Q}$ são:

$$\mathbb{Q} = \theta(G), M = \theta(\{e\}), \mathbb{Q}[\alpha_1] = \theta(A_1), \mathbb{Q}[\alpha_2] = \theta(A_2), \mathbb{Q}[\alpha_3] = \theta(A_3)$$

e finalmente $\mathbb{Q}[\sqrt{3}\, i] = \theta(B)$. Entre esses, apenas $\mathbb{Q}, M$ e $\theta(B)$ são extensões normais de $\mathbb{Q}$.

EXEMPLO 2. $M = \text{Gal}(x^7 - 1, \mathbb{Q})$. Sabemos que se $\zeta$ é uma raiz primitiva 7-ésima da unidade temos:
$M = \mathbb{Q}[\zeta]$ e $[M : \mathbb{Q}] = 6$. Portanto se $G = \text{Aut}_{\mathbb{Q}} M$ temos $|G| = 6$. Porém por um exercício anterior temos que $G$ é abeliano, logo $G \simeq \mathbb{Z}_6$ grupo cíclico de ordem 6.

Assim, como $G$ é cíclico de ordem 6 existem apenas 4 subgrupos de $G$, $\{e\}, G, A$ e $B$ onde $|A| = 3$ e $|B| = 2$ e teremos,

$$\mathscr{I}(M, \mathbb{Q}) = \{M, \mathbb{Q}, \theta(A), \theta(B)\}.$$

Como $G$ abeliano todos os corpos $L \in \mathscr{I}(M, \mathbb{Q})$ são normais sobre $\mathbb{Q}$.

Os elementos de $G$ ficam determinados por:

$$e:\zeta \to \zeta$$
$$\sigma_1:\zeta \to \zeta^2$$
$$\sigma_2:\zeta \to \zeta^3$$
$$\sigma_3:\zeta \to \zeta^4$$
$$\sigma_4:\zeta \to \zeta^5$$
$$\sigma_5:\zeta \to \zeta^6$$

os subgrupos $A$ e $B$ são:

$$A = \{e, \sigma_1, \sigma_3\} \text{ e } B = \{e, \sigma_5\}$$

e finalmente os elementos de $\mathscr{I}(M, \mathbb{Q})$ são $\mathbb{Q} = \theta(G)$, $M = \theta(\{e\})$, $\theta(A) = \mathbb{Q}[u]$ onde $u = \zeta + \zeta^2 + \zeta^4$ e $\theta(B) = \mathbb{Q}[v]$ onde $v = \zeta + \zeta^6$.

EXEMPLO 3. Seja $M = \mathrm{Gal}(x^4 - 2, \mathbb{Q})$. Sabemos que $G = \mathrm{Aut}_{\mathbb{Q}} M \simeq \simeq D_4$ e que os elementos de $G$ são determinados pelos efeitos sobre $\alpha = \sqrt[4]{2} \in \mathbb{R}$ e $i = \sqrt{-1} \in \mathbb{C}$, segundo o quadro abaixo:

| | $e$ | $\sigma_2$ | $\sigma_3$ | $\sigma_4$ | $\sigma_5$ | $\sigma_6$ | $\sigma_7$ | $\sigma_8$ |
|---|---|---|---|---|---|---|---|---|
| $\alpha \to$ | $\alpha$ | $\alpha$ | $-\alpha$ | $-\alpha$ | $\alpha i$ | $\alpha i$ | $-\alpha i$ | $-\alpha i$ |
| $i \to$ | $i$ | $-i$ | $i$ | $i$ | $i$ | $i$ | $i$ | $-i$ |

os subgrupos de $G$ e os corpos intermediários são (verifique isto)

ordem $8: G \simeq D_4$ — $\theta(G) = \mathbb{Q}$

ordem $4: A_1 = \{e, \sigma_5, \sigma_5^2, \sigma_5^3\} \simeq \mathbb{Z}_4$ — $\theta(A_1) = \mathbb{Q}[i]$

$A_2 = \{e, \sigma_5^2, \sigma_2, \sigma_5^2\sigma_2\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ — $\theta(A_2) = \mathbb{Q}[\sqrt{2}]$

$A_3 = \{e, \sigma_5^2, \sigma_5\sigma_2, \sigma_5^3\sigma_2\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ — $\theta(A_3) = \mathbb{Q}[i\sqrt{2}]$

ordem $2: B_1 = \{1, \sigma_5^2\} = \mathbb{Z}(G) \simeq \mathbb{Z}_2$ — $\theta(B_1) = \mathbb{Q}[i, \sqrt{2}]$

$B_2 = \{1, \sigma_2\} \simeq \mathbb{Z}_2$ — $\theta(B_2) = \mathbb{Q}[\alpha]$

$B_3 = \{1, \sigma_5\sigma_2\} \simeq \mathbb{Z}_2$ — $\theta(B_3) = \mathbb{Q}[(1+i)\alpha]$

$B_4 = \{1, \sigma_5^2\sigma_2\} \simeq \mathbb{Z}_2$ — $\theta(B_4) = \mathbb{Q}[i\alpha]$

$B_5 = \{1, \sigma_5^2\sigma_2\} \simeq \mathbb{Z}_2$ — $\theta(B_5) = \mathbb{Q}[(1-i)\alpha]$

ordem $1: \{e\}$ — $\theta(\{e\}) = M$

Os corpos intermediários que são normais sobre $\mathbb{Q}$ são: $\mathbb{Q}, M$, $\theta(A_1), \theta(A_2), \theta(A_3)$ e $\theta(B_1)$.

## EXERCÍCIOS

1. Seja $M = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Prove que:
   a) $M \supset \mathbb{Q}$ é galoisiana.
   b) $G = \mathrm{Aut}_{\mathbb{Q}} M \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$
   e use a correspondência de Galois para calcular todos os elementos de $\mathscr{I}(M, \mathbb{Q})$ e de $\mathscr{S}(G)$.

2. Seja $M = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$. Prove que:
   a) $M \supset \mathbb{Q}$ é galoisiana
   b) $G = \mathrm{Aut}_{\mathbb{Q}} M = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
   e use a correspondência de Galois para calcular todos os elementos de $\mathscr{I}(M, \mathbb{Q})$ e de $\mathscr{S}(G)$.

3. Seja $M = \mathrm{Gal}(x^5 - 2, \mathbb{Q})$ e $K = \mathbb{Q}[\zeta]$ onde $\zeta$ é uma raiz quinta, primitiva, da unidade.
   a) Prove que $M \supset K$ é galoisiana e calcule $G = \mathrm{Aut}_K M$.
   b) Use a correspondência de Galois para calcular os elementos de $\mathscr{I}(M, K)$ e de $\mathscr{S}(G)$.

4. Mesmo exercício do item anterior para a extensão $M = \mathrm{Gal}(x^6 - 3, \mathbb{Q})$, $K = \mathbb{Q}[\zeta]$ onde $\zeta$ é uma raiz sexta, primitiva, da unidade.

5. a) Se $L_1$ e $L_2$ são subcorpos de um corpo $M$, definimos, $\langle L_1, L_2 \rangle$ como a interseção de todos os subcorpos de $M$ contendo $L_1$ e $L_2$. Prove que: $\langle L_1, L_2 \rangle$ é o menor subcorpo de $M$ contendo $L_1$ e $L_2$.
   b) Se $H_1$ e $H_2$ são subgrupos de um grupo $G$, definimos, $\langle H_1, H_2 \rangle$ como a interseção de todos os subgrupos de $G$ contendo $H_1$ e $H_2$. Prove que: $\langle H_1, H_2 \rangle$ é o menor subgrupo de $G$ contendo $H_1$ e $H_2$.

6. Seja $M \supset K$ uma extensão galoisiana. Prove que: (usando as notações do último parágrafo)
   a) se $L_1, L_2 \in \mathscr{I}(M, K)$ então $\psi(\langle L_1, L_2 \rangle) = \psi(L_1) \cap \psi(L_2)$
   b) se $H_1, H_2 \in \mathscr{S}(G)$, $G = \mathrm{Aut}_K M$ então,
   $$\theta(\langle H_1, H_2 \rangle) = \theta(H_1) \cap \theta(H_2).$$

7. Seja $M = \mathrm{Gal}(x^4 - 3x^2 + 4, \mathbb{Q})$. Estude $\mathscr{I}(M, \mathbb{Q})$ e $\mathscr{S}(G)$, $G = \mathrm{Aut}_{\mathbb{Q}} M$ através da correspondência de Galois.

8. Mesmo exercício do item anterior para a extensão $M = \mathrm{Gal}(x^4 - 3, \mathbb{Q}[i]) \supset K = \mathbb{Q}[i]$.

9. Seja $L$ uma extensão galoisiana sobre $K$ de grau $[L:K] = p^m \cdot q$ onde $p$ e $q$ são primos.
Prove que se $p \geq q$ então existe uma extensão $N \in \mathscr{I}(L, K)$ tal que $N \supset K$ é normal, e $[N:K] = q$. (use Teorema de Sylow e correspondência de Galois).
10. Seja $L \supset K$ uma extensão galoisiana tal que $[L:K] = p^m \cdot n$ onde $p$ é primo e $p \nmid n$. Prove que $\exists\, N \in \mathscr{I}(L, K)$ tal que $[N:K] = n$ (use Teorema de Sylow e correspondência de Galois).
11. Seja $L \supset K$ uma extensão galoisiana tal que $[L:K] = p^m$ onde $p$ é um número primo. Prove que $\exists\, N_1, N_2, \ldots, N_m = L \in \mathscr{I}(L, K)$ tais que: $[N_i:K] = p^i$ e mais: $K \subset N_1 \subset N_2 \subset \ldots \subset N_i \subset N_{i+1} \subset \subset \ldots \subset L$ onde $N_i \supset K$ normal $\forall\, i \in \{1, 2, \ldots, m\}$.

## §3 Solubilidade por meio de radicais

Neste parágrafo vamos definir rigorosamente a noção de polinômio solúvel por meio de radicais, e daremos um critério (através dos grupos de automorfismos) para que as raízes de um polinômio sejam expressas por meio de radicais.

Por exemplo, suponhamos que uma raiz $\alpha$ de $f(x) \in \mathbb{Q}[x]$ seja expressa por meio dos seguintes radicais:

$$\alpha = \frac{\sqrt[5]{2 - \sqrt[3]{2}} + \sqrt{3}}{\sqrt[7]{1 - \sqrt[4]{5}}}.$$

se denotarmos $a_1 = \sqrt[4]{5}$, $a_2 = \sqrt[7]{1 - a_1}$, $a_3 = \sqrt[3]{2}$, $a_4 = \sqrt[5]{2 - a_3}$, $a_5 = \sqrt{3}$, teremos:

$$\mathbb{Q} = K_0 \subseteq K_0[a_1] = K_1 \subseteq K_1[a_2] = K_2 \subseteq K_2[a_3] = \\ = K_3 \subseteq K_3[a_4] = K_4 \subseteq K_4[a_5] = K_5.$$

Mais ainda, $a_1^4 \in K_0$, $a_2^7 \in K_1$, $a_3^3 \in K_2$, $a_4^5 \in K_3$ e $a_5^2 \in K_4$, $\alpha \in K_5 = \mathbb{Q}[a_1, a_2, a_3, a_4, a_5]$.

Assim dada a expressão radical acima conseguimos uma extensão $K_5$, contendo $\alpha$, com certas propriedades.

Vamos agora definir a noção de extensão radical. Dizemos que $M \supset K$ finita é uma extensão radical sobre $K$ se $\exists\, a_1, a_2, \ldots, a_r \in M$ tais que:

(a) $K = K_0 \subseteq K_1 = K[a_1] \subseteq K_2 = K_1[a_2] \subseteq \ldots \subseteq K_i = = K_{i-1}[a_1] \subseteq \ldots \subseteq K_r = M.$

(b) $\forall\, i \in \{1, 2, \ldots, r\}$ $\exists\, n_i \in \mathbb{N}$ tais que $a_i^{n_i} \in K_{i-1}$.

Observe que como $a_i^{n_i} = b_{i-1} \in K_{i-1}$ podemos também denotar $K_i = k_{i-1}[\sqrt[n_i]{b_{i-1}}]$, ou seja $K_i$ é obtido de $K_{i-1}$ por adjunção de uma raiz do polinômio $x^{n_i} - b_{i-1} \in K_{i-1}[x]$.

Agora, se $f(x) \in K[x]$ e uma raiz $\alpha$ de $f(x)$ está numa extensão radical $M = K[a_1, a_2, \ldots, a_r]$ como acima, então:
$\alpha$ pode ser expresso como uma expressão polinomial $p(a_1, a_2, \ldots, a_r)$ com coeficientes em $K$, isto é,

$$\alpha = p(a_1, a_2, \ldots, a_r) \in K[a_1, a_2, \ldots, a_r].$$

Mantendo a notação acima: $a_1 = \sqrt[n_1]{b_0}$, $a_2 = \sqrt[n_2]{b_1}, \ldots,$ $a_r = \sqrt[n_r]{b_{r-1}}$ onde $b_j \in K_j$, $j = 0, 1, \ldots, r-1$ e teremos também:

$$\alpha = p(\sqrt[n_1]{b_0}, \sqrt[n_2]{b_1}, \ldots, \sqrt[n_r]{b_{r-1}}),$$

que é uma expressão polinomial radical.
Observe que,

$$a_1 = \sqrt[n_1]{b_0},\ a_2 = \sqrt[n_2]{q_1(\sqrt[n_1]{b_0})},\ a_3 = \sqrt[n_3]{q_2(\sqrt[n_2]{q_1(\sqrt[n_1]{b_0})})},$$

etc., etc., ... onde $q_1, q_2, \ldots$ são polinômios com coeficientes em $K$, e assim $\alpha$ poderia se reduzir a uma expressão radical envolvendo polinômios e raízes de $b_0 \in K$.

Observe também que existe extensões radicais, como $M = \mathbb{Q}[\sqrt[3]{2}]$, que não são normais e vice-versa, se $L = \text{Gal}(x^3 - 3x - 1, \mathbb{Q})$ então como as 3 raízes de $x^3 - 3x - 1$ são reais segue (prove isto) que $[L:\mathbb{Q}] = 3$ e $L$ não é uma extensão radical de $\mathbb{Q}$.

Agora vamos definir a noção de polinômio solúvel por meio de radical.

Seja $f(x) \in K[x]$ e $L = \text{Gal}(f, K)$. Dizemos que $f(x)$ é um *polinômio solúvel por meio de radicais sobre* $K$ se $\exists$ uma extensão radical $M \supset K$ tal que $M \supset L \supset K$.

Pelas observações anteriores as raízes $\alpha \in L \subset M$ poderão ser expressas como polinômios envolvendo certos radicais.

Antes de demonstrarmos o principal teorema desse parágrafo, vamos demonstrar a seguinte proposição.

PROPOSIÇÃO 7. *Seja $L \supset K \supset \mathbb{Q}$ uma extensão radical sobre $K$. Então existe uma extensão $M \supset L \supset K$ tal que $M$ é radical e Galoisiana sobre $K$.*

*Demonstração*: Como $L \supset K$ é uma extensão radical podemos escrever

$$K = L_0 \subset L_1 \subset \ldots \subset L_{r-1} \subset L_r = L$$

onde

$$L_i = L_{i-1}[\alpha_i], \ \alpha_i \text{ raiz de } x^{n_i} - a_i \in L_{i-1}[x].$$

Seja $n = n_1 \cdot n_2 \cdot \ldots \cdot n_r$ e $\zeta$ uma raiz primitiva $n$-ésima da unidade. Substituindo, se necessário, $L$ por $L[\zeta]$ e $K$ por $K[\zeta]$ podemos assumir que $L \supset K$ e $K$ contém as raízes $n$-ésimas da unidade.

Assim $L_1 \supset L_0 = K$ é normal pois contém $\alpha_1$ raiz de $x^{n_1} - a_1 \in K[x]$, e $K$ contém as raízes $n_1$-ésimas da unidade. De fato, temos $L_1 = \text{Gal}(x^{n_1} - a_1, K)$.

Seja $g_1(x) = \prod_{\sigma \in \text{Aut}(L_1/K)} (x^{n_2} - \sigma(a_2))$. Pelo Teorema 3 temos que $g_1(x) \in K[x]$. Agora, juntando-se todas as raízes dos polinômios $x^{n_1} - a_1$, e $g_1(x)$ ao corpo $K$ conseguimos uma extensão galoisiana $L_2^* \supset K$ onde $L_2^* \subset L_1$. Seguindo indutivamente esse processo conseguimos a desejada extensão $M$.

TEOREMA 5. *Sejam $K \supset \mathbb{Q}$, $f(x) \in K[x]$ e $L = Gal(f, K)$. Se $f(x)$ é solúvel por meio de radicais sobre $K$ então o grupo $G = Aut_K\, L$ é solúvel.*

*Demonstração.* Pela Proposição 7 existe $M \supset L \supset K$ tal que $M$ é radical e galoisiana sobre $K$.

Assim como $L \supset K$ é normal segue pelo teorema fundamental de Galois que:

$$G = \text{Aut}_K L \simeq \text{Aut}_K M / \text{Aut}_L M$$

Portanto será suficiente provarmos que $\text{Aut}_K M$ é solúvel.

Agora, consideremos $\zeta$ uma raiz primitiva $n$-ésima da unidade, onde:

$$n = n_1 \cdot n_2 \ldots n_r, \ M = K[a_1, a_2, \ldots, a_r]$$

e $a_i^{n_i} \in K_{i-1}, K_i = K_{i-1}[a_i]$ como nas notações anteriores.

Considerando $M^* = M[\zeta], K^* = K[\zeta]$ e se $\sigma \in \text{Aut}_K M$ consideramos,

$$\sigma^* \in \text{Aut}_{K^*} M^*$$

tal que:

$$\sigma^*|_M = \sigma \text{ e } \sigma^*(\zeta) = \zeta.$$

Claramente se $\sigma \neq \tau$ temos $\sigma^* \neq \tau^*$ e portanto a função abaixo

$$\begin{aligned} \Phi\colon \mathrm{Aut}_K M &\to \mathrm{Aut}_{K^*} M^* \\ \sigma &\rightsquigarrow \sigma^* \end{aligned}$$

define um homomorfismo injetivo. Daí segue que $\mathrm{Aut}_K M \simeq \Phi(\mathrm{Aut}_K M) \leq$ $\leq \mathrm{Aut}_{K^*} M^*$ e portanto $\mathrm{Aut}_K M$ será solúvel se $\mathrm{Aut}_{K^*} M^*$ for solúvel.

Assim podemos assumir que $K$ contém uma raiz primitiva $n$-ésima, $\zeta$, da unidade.

Agora,

se $M = K[a_1, a_2, \ldots, a_r]$ é uma extensão radical sobre $K, n = n_1 \cdot n_2 \cdot \ldots n_r$, onde $a_i^{n_i} \in K_{i-1}$, e $K$ contém uma raiz primitiva $n$-ésima da unidade, vamos provar por indução sobre $r$ que $\mathrm{Aut}_K M$ é um grupo solúvel.

Se $r = 1$, então $M = K[a_1]$, $a_1^{n_1} = b_0 \in K$ e como $K$ contém uma raiz primitiva $n_1$-ésima da unidade segue que $M = \mathrm{Gal}(x^{n_1} - b_0, K)$ e $\mathrm{Aut}_K M$ é um grupo abeliano (veja Proposição 4).

Pela hipótese de indução vamos admitir que $\mathrm{Aut}_{K_1} M$ é solúvel onde $M = K_1[a_2, a_3, \ldots, a_r]$.

Como $K_1 = \mathrm{Gal}\,(x^{n_1} - b_0, K)$ é normal sobre $K$ a função $\psi\colon \mathrm{Aut}_K M \to \mathrm{Aut}_K K_1$ define um homomorfismo (de grupos) cujo nú-
$\sigma \rightsquigarrow \sigma|_{K_1} = \sigma_1$
cleo $N(\psi) = \mathrm{Aut}_{K_1} M$.

Assim, pelo teorema de isomorfismo, temos:

$$\mathrm{Aut}_K M/\mathrm{Aut}_{K_1} M \simeq \psi(\mathrm{Aut}_K M) \leq \mathrm{Aut}_K K_1$$

Como $\mathrm{Aut}_K K_1$ é abeliano e por indução $\mathrm{Aut}_{K_1} M$ é solúvel então temos que $\mathrm{Aut}_K M$ é solúvel e isto demonstra o teorema. ■

COROLÁRIO. *O polinômio $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ não é solúvel por meio de radicais sobre $\mathbb{Q}$.*

*Demonstração.* Sabemos pelo corolário da Proposição 5 que $\mathrm{Aut}_{\mathbb{Q}} L \simeq S_5$ não solúvel, onde $L = \mathrm{Gal}(f, \mathbb{Q})$, e o resultado segue imediatamente. ■

Vamos encerrar o capítulo com o exemplo do polinômio geral de grau $n$.

EXEMPLO. Seja $L = \mathbb{Q}(x_1, x_2, \ldots, x_n)$ o corpo das funções racionais com coeficientes sobre $\mathbb{Q}$ nas "variáveis independentes $x_1, x_2, \ldots, x_n$".

Se definimos:

$$s_1 = x_1 + x_2 + \dots + x_n$$
$$s_2 = x_1x_2 + x_1x_3 + \dots + x_1x_n + \dots + x_{n-1}x_n$$
$$\vdots$$
$$s_n = x_1 x_2 \cdots x_n$$

então $K = \mathbb{Q}(s_1, s_2, \dots, s_n)$ é chamado o corpo das funções racionais simétricas sobre $\mathbb{Q}$.

Agora é fácil ver que $x_1, x_2, \dots, x_n$ são elementos algébricos sobre $K$ (embora transcendentes sobre $\mathbb{Q}$) pois $L = \mathrm{Gal}(f, K)$ onde

$$f(t) = t^n - s_1t^{n-1} + s_2t^{n-2} + \dots + (-1)^n s_n \in K[t].$$

Assim, $x_1, \dots, x_n$ são as $n$ raízes de $f(t)$ e mais, $L = K[x_1, x_2, \dots, x_n] = \mathrm{Gal}(f, K)$.

Pode-se provar (verifique isto) que cada permutação $\sigma_0$ do conjunto $\Omega = \{x_1, x_2, \dots, x_n\}$ das raízes de $f$ dá origem a um elemento $\sigma \in \mathrm{Aut}_K L$, ou seja, $[L:K] = n!$ e $\mathrm{Aut}_K L \simeq S_n$.

O polinômio $t^n - s_1t^{n-1} + \dots + (-1)^n s_n = f(t)$ chama-se o *polimio geral de grau n sobre* $\mathbb{Q}$ e portanto:

O polinômio geral de grau $n$ sobre $\mathbb{Q}$, $n \geq 5$, não é solúvel por meio de radicais sobre o corpo das funções racionais simétricas.

## EXERCÍCIOS

1. Prove que os seguintes polinômios $f(x) \in \mathbb{Q}[x]$ não são solúveis por meio de radicais sobre $\mathbb{Q}$:
   a) $f(x) = x^5 - 20x^2 + 5$
   b) $f(x) = x^5 - 4x + 2$
   c) $f(x) = x^5 - 4x^2 + 2$
   d) $f(x) = x^5 - 6x^2 + 3$
   e) $f(x) = x^7 - 10x^5 + 15x + 5$
2. Resolva a equação $t^6 + 2t^5 - 5t^4 + 9t^3 - 5t^3 + 2t + 1 = 0$ por meio de radicais $\left(\text{sugestão: } u = t + \dfrac{1}{t}\right)$.
3. Prove que:
   se $p(x) \in K[x]$ é irredutível sobre $K$ e uma raiz de $p(x)$ é expressa por meio de radicais, então $p(x)$ é solúvel por meio de radicais.
4. Determine extensões radicais sobre $\mathbb{Q}$ contendo os seguintes elementos de $\mathbb{C}$.
   a) $\dfrac{(\sqrt[7]{13} - \sqrt{5})}{\sqrt[4]{2}}$ b) $(\sqrt{2} + 2\sqrt[3]{3})^4$.

# REFERÊNCIAS

1. B. L. Van der Waerden, Modern Algebra, vol. I – Frederick Ungar Publishing Co, New York, 1949.
2. G. Birkhoff & S. Mac Lane, A Survey on Modern Algebra, The MacMillan Company, 1941.
3. Ian Stweart. Galois Theory.
4. I. Kaplansky, Introdução a Teoria de Galois, Notas de Matemática n.º 13 – IMPA – 1958.
5. I. N. Herstein, Topics in Algebra, Blaisdell Publishing Company, 1964.
6. J. Rotman, Allyn & Bacon, The Theory of Groups, and introduction, Inc. 1965.
7. L. H. Jacy Monteiro, Elementos de Algebra, Elementos de Matemática, IMPA, 1969.
8. S. Lang, Algebraic Structures, Addison-Wesley Publishing Company, 1968.

# ÍNDICE ALFABÉTICO

adilson gonçalves

Nasceu em Bangu, RJ, onde fez seus estudos primário e secundário, soltou pipas e jogou muita pelada, chegando a ser um ponta direita razoável, embora hoje não passe de um torcedor do Flamengo. Na matemática, foi bem mais longe. Depois de licenciar-se pela então Faculdade Nacional de Filosofia, obteve o grau de Mestre pelo IMPA, e de Doutor pela Universidade de Chicago. Trabalha em Álgebra, mais precisamente em Teoria dos Grupos. Foi professor na Universidade de Brasília, na Universidade Federal do Rio de Janeiro e atualmente pertence à Universidade Federal de Pernambuco. É autor de um texto sobre Representação de Grupos e co-autor de outro sobre Álgebra Linear.

introdução à álgebra

CNPq Conselho Nacional de Desenvolvimento Científico e Tecnológico

Instituto de Matemática Pura e Aplicada